groupement français de l'industrie de l'information

e-réputation et identité numérique des organisations

Typologie des menaces et identification des modes de traitement applicables

« Il faut vingt ans pour construire une réputation, cinq minutes pour la détruire ».
Warren Buffett

GROUPE DE TRAVAIL INTELLIGENCE ECONOMIQUE ET ECONOMIE DE LA CONNAISSANCE

15 avril 2010

A propos du GFII (http://www.gfii.asso.fr)

Le GFII regroupe les principaux acteurs du marché de l'information et de la connaissance.

Le GFII anime des groupes de travail, qui permettent aux acteurs de l'industrie de l'information et de la connaissance de se rencontrer, de confronter et d'échanger leurs points de vue sur les aspects juridiques, techniques et économiques du secteur.

Pour valoriser ces travaux, le GFII organise des journées d'étude et publie des ouvrages de référence. Il propose également des voyages d'étude en France et à l'étranger (salon Online Information de Londres, Foire du Livre de Francfort).

Le GFII a créé en 2010 un réseau social pour ses membres (AMICO, les Acteurs du Marché de l'Information et de la COnnaissance). Via ce réseau, l'association diffuse des analyses sur le marché de l'information, *La Dépêche du GFII*, et une veille sur l'actualité du secteur, *GFII 360*.

Le GFII est co-organisateur d'i-expo, le salon de l'Information stratégique, de la veille et de l'Intelligence économique, qui se déroulera les 9 et 10 juin 2010 (http://www.i-expo.net).

e-réputation et identité numérique des organisations

Typologie des menaces et identifications des modes de traitement applicables

Préambule

La gestion de l'identité numérique, appelée également e-réputation, constitue aujourd'hui un enjeu essentiel pour une entreprise, quel que soit son secteur d'activité. En effet, une atteinte à la réputation est susceptible d'avoir un impact très négatif sur le résultat d'une entreprise et peut même dans certains cas entraîner sa faillite. Les exemples sont hélas nombreux d'entreprises mal préparées à la gestion de telles crises qui n'ont su ni anticiper leur apparition, ni en maîtriser les effets, du moins autant que faire se peut.

L'explosion des sources numériques avec l'avènement d'Internet et aujourd'hui du Web 2.0 a complètement transformé l'univers de la communication d'entreprise. Une rumeur sur une société ou un produit peut se propager en quelques heures dans le monde entier, faisant parfois plonger le cours de bourse d'une entreprise de 20% en une journée ; une action de dénigrement peut entacher l'image d'une entreprise durant plusieurs années ; des critiques de consommateurs sur un produit peuvent en faire chuter les ventes. Le virtuel impacte le réel et surtout l'économie.

Par la réalisation de ce guide, le GFII (Groupement Français de l'Industrie de l'Information), a souhaité concevoir un outil destiné aux dirigeants d'entreprises et aux cadres concernés par ce sujet, afin de les accompagner dans la gestion de crises portant atteinte à l'identité numérique de leur société.

Après une introduction des concepts et des enjeux liés à la thématique, ce guide propose des fiches pratiques reprenant les principales menaces qui ont pu être identifiées et présente pour chacune d'entre elles une description de ses caractéristiques puis les modes de traitement applicables. Chaque fiche est également illustrée d'un ou deux exemples réels mais anonymisés assorti d'un focus assez précis sur les modes de traitement mis en place et sur les actions mises en œuvre par les différents services de l'entreprise.

Ensuite, des préconisations de mesures préventives et curatives seront présentées et complétées d'un panorama d'acteurs susceptibles d'accompagner les décideurs dans les actions à mener.

L'objectif n'est en aucun cas d'apporter des réponses précises aux problèmes particuliers qu'une entreprise peut rencontrer mais de fournir des pistes de réflexion permettant de mieux comprendre l'événement pour ensuite identifier les professionnels à solliciter pour résoudre la crise.

La rédaction collective de ce guide s'est faite dans le cadre des travaux du Groupe Intelligence Economique et Economie de la Connaissance du GFII.

Les rédacteurs sont à la fois des professionnels du domaine de l'information professionnelle exerçant dans des sociétés du secteur qui sont amenées à fournir des produits et prestations de services à des entreprises clientes qui souhaitent sécuriser ou encore valoriser leur réputation numérique ; mais aussi des utilisateurs de produits d'information. Les rédacteurs :

- Antoine Montoux, KB Crawl,
- Antoine Raulin, Bureau van Dijk Information Management,
- Caroline Martin, Cemagref,
- Céline Molina, Spotter,
- Christophe Asselin, Digimind,
- Christophe Marnat, AMI Software,
- Emmanuelle Jannès-Ober, Cemagref,
- Floriane Giovannini, Cemagref,
- Frédéric Martinet, Actulligence Consulting,
- Jérôme Cail, Lexis-Nexis,
- Julien Flandrois, KB Crawl,
- Ludovic Bour, ACFCI,
- Marc Michiels, Argus de la presse,
- Muriel de Boisseson, Dow Jones,
- Olivier Guy, Argus de la Presse,
- Patrick Baldy, CEA,
- Philippe Plazanet, Crédit Agricole S.A,
- Ruth Martinez, GFII.

Le groupe de travail Intelligence Economique et Economie de la Connaissance traite plus particulièrement des outils et solutions d'accès et de traitement de l'information. Il est piloté par Christophe Marnat, directeur du développement de la société AMI Software.

Le Groupement Français de l'Industrie de l'Information (GFII) remercie chaleureusement Maître Haas pour la richesse de sa contribution sur le thème des recours légaux.

Sommaire

I. Présentation des concepts et des enjeux

A. Définitions des concepts

1. Le risque de réputation

La réputation relève de l'opinion émise par le public envers une personne, un groupe ou une organisation. C'est une perception des parties prenantes qui intègre également la notion de notoriété. Elle est soit positive, soit négative. Elle est plus rarement neutre ou bien dans ce cas elle témoigne d'un déficit de notoriété.

Warren Buffett, financier renommé, deuxième homme le plus riche du monde, surnommé l'Oracle d'Omaha, aurait un jour déclaré : « il faut vingt ans pour construire une réputation, cinq minutes pour la détruire ». Cette affirmation met en évidence la fragilité de la réputation qui n'est jamais complètement établie et peut être aisément altérée par de multiples facteurs.

L'individu et l'entreprise sont intimement liés dans la mesure où les actions d'un individu ont un impact sur son entreprise et vice versa.

Le risque de réputation quand il engage les entreprises prend souvent une dimension économique. En effet, une atteinte à la réputation peut avoir un effet dévastateur sur l'environnement de l'entreprise et modifier les relations des partenaires, clients, salariés vis-à-vis de l'entreprise incriminée.

La calomnie, la rumeur, la désinformation, la manipulation ou la propagande ne sont pas des notions nouvelles dans ce monde. Depuis que l'homme pense et vit en communauté, ces phénomènes existent.

Néanmoins, aujourd'hui, la caisse de résonnance est décuplée par la vitesse de propagation des informations notamment des rumeurs, la dimension des espaces touchés (le monde) et le nombre de personnes exposées. Le Web étant un réseau mondialisé (le « village planétaire ») ce phénomène de réputation négative sur le net est plus sensible que jamais et est devenu progressivement une préoccupation majeure. Si, au départ les internautes avaient une attitude responsable (vision libertaire angéliste des débuts de l'Internet), l'évolution du Web 2.0 où l'internaute devient le centre du réseau en étant auteur de contenu (*User Generated Content*), a engendré une croissance exponentielle de la masse informationnelle. Enfin, les systèmes de syndication (fils RSS) permettent une vitesse de propagation inégalée, vitesse encore renforcée par les outils de microblogging.

2. e-réputation

La e-réputation encore appelée cyber-réputation, Web-réputation ou réputation numérique recouvre deux concepts principaux très larges que sont la réputation et la dimension Internet / « en ligne ». C'est donc l'image d'une personne physique ou morale façonnée par l'ensemble des opinions émises sur les réseaux numériques tels qu'Internet.

Cette perception se compose des éléments générés par l'individu ou l'entreprise concernés et des données produites par les acteurs de son environnement (consommateurs, experts, …). La

spécificité d'Internet est qu'une grande partie de la génération des contenus échappe à l'entreprise et constitue pour cette raison une opportunité ou un risque.

Le Web offre différents supports de communication en ligne : blogs, forums, sites multimédia, réseaux sociaux, sites Web qui ont leurs spécificités et offrent une dimension participative plus ou moins importante. Ce qui change avec la dimension Internet est le délai d'accès à l'information. Il devient encore plus court avec l'émergence de services de microblogging tels que Twitter. L'audience s'élargit aussi considérablement car ces médias peuvent virtuellement atteindre toute personne dans le monde, dotée d'un accès Internet. L'information peut désormais se propager sur des millions de pages et chaque internaute devient un éditeur/ contributeur potentiel. Le journaliste, l'analyste, le blogueur cohabitent ; la crédibilité et la fiabilité de leurs écrits sont généralement peu remises en cause sur le Web.

Sur Internet, le bouche à oreille devient le « buzz » et la vitesse de propagation des messages est démultipliée.

L'Internet est devenu le lieu où se font et se défont les réputations. Dire publiquement du mal d'autrui a toujours existé, mais l'oubli était généralement de mise. Au contraire, la mémoire persistante du Web fait que tout reste (pour la plupart) en ligne accessible via les moteurs de recherche (ne dit-on pas que le Web est le fonds d'archives le plus vaste).

Pour essayer de contrôler sa réputation sur Internet encore faut-il connaître les vecteurs à surveiller, chaque année plus nombreux : les sites institutionnels, les blogs, les forums, les réseaux sociaux, les wikis, les plateformes vidéo, les agrégateurs d'actualité, les sites communautaires...

3. Identité numérique

L'*homo Internetus* n'est plus un *homo anonymous* ! Sur la toile le droit à l'anonymat n'existe pas dans les faits.

On a souvent évoqué à propos d'Internet le célèbre cartoon : ***« On the Internet, nobody knows you're a dog »*** (« Sur l'Internet, personne ne sait que tu es un chien »). Cette caricature de Peter Steiner parue dans le *New Yorker* du 5 juillet 1993 illustre l'anonymat existant sur Internet à l'époque. Elle représente un chien assis sur une chaise devant un bureau, qui utilise un ordinateur tout en prononçant ces paroles à un autre chien se tenant assis par terre à côté de lui[1].

L'avènement du Web 2.0 dans les années 2000 et la multiplication des réseaux sociaux, blogs ou wikis permettent désormais aux internautes d'interagir avec le contenu des pages mais aussi entre eux. Chaque utilisateur dispose d'une véritable identité numérique constituée d'informations diverses, volontairement diffusées ou non, laissées sur la toile puis archivées dans des moteurs de recherche. Ces « traces » numériques, informations, interactions sont indélébiles pour la plupart et accessibles librement par tous. Il y a un niveau de confiance implicite car ces données pourraient être utilisées à des fins commerciales, voire frauduleusement dans le cadre d'une usurpation d'identité.

1. **Source : http://www.cartoonbank.com/item/22230**

L'identité numérique est constituée d'informations personnelles : qui vous êtes, comment vous vous présentez, les personnes que vous connaissez, ce que vous possédez et ce que vous faites. A ces données précises et factuelles, il faut ajouter l'image sociale projetée. Elle est aussi liée à l'expression de la personnalité de chacun et résulte de l'interprétation des autres. Tous ces éléments sont dispersés sur la toile.

Les enjeux autour de l'identité numérique recouvrent des risques liés à la sécurité, à la protection de la vie privée, à des questions éthiques et à des considérations économiques.

Comme la réputation, l'identité n'est pas figée. Elle évolue et se transforme dynamiquement au gré des interactions. Il peut y avoir un décalage considérable entre l'identité *online* (numérique) et *offline* (dans le monde réel) car certaines personnes peuvent avoir une approche fractionnée et utiliser de multiples identités en fonction de leurs différentes utilisations (personnelle, professionnelle..) et des réseaux fréquentés. Il est toujours possible d'utiliser des outils technologiques pour naviguer de façon anonyme.

Une meilleure gestion de son identité numérique passe aussi par la meilleure connaissance des outils et technologies en présence. Les priorités sont de surveiller ses propres traces et ce qui se dit de soi.

B. Les enjeux pour une organisation (entreprise, association, administration)

Gérer son image virtuelle est devenue une nécessité pour une organisation. Les enjeux d'ordres économique et stratégique sont très importants et dépassent largement la problématique de la stratégie de communication.

Les conséquences d'une e-réputation dégradée peuvent se constater à tous les niveaux : baisses des ventes, détérioration de la relation clients, impact sur le moral des employés et donc leur productivité. Les relais tels que les syndicats, les ONG, les associations de défense des consommateurs, la presse, les groupes d'influence peuvent participer à cette e-réputation négative et contribuer à sa diffusion.

La réputation d'une entreprise est donc complexe et englobe de nombreux paramètres. À la qualité des produits et des services, la gestion des ressources humaines et la valeur de la marque, il convient d'ajouter aujourd'hui la responsabilité sociale de l'entreprise et les valeurs de citoyenneté.

Source : Dow Jones and Company

Les conséquences d'une altération de cette image peuvent engager l'existence même de l'entreprise à court terme. Notamment sa structure financière peut être totalement bousculée en quelques heures suite à une rumeur ou une mauvaise information diffusée sur le Net (affaire

Apple/engadget[2]). L'Autorité des Marchés Financiers (AMF) a d'ailleurs produit une fiche de recommandations quant à la diffusion d'informations financières sur le Web pour rappeler certaines règles juridiques concernant la diffusion d'informations fausses[3].

La question se révèle cruciale d'autant que les réponses juridiques trouvent rapidement leurs limites face au contexte mondialisé du Web. Les réponses, consistant alors à mettre en place des stratégies de référencement de crise ou de "pousser" des contenus positifs pour noyer les commentaires négatifs, ne sont souvent que des pis-aller.

En général, l'e-réputation doit se gérer en amont. Car retravailler une image détériorée est une œuvre de longue haleine. On parle alors pour les entreprises d'entrer "dans une logique de co-création de sa propre e-réputation".

Les collectivités locales sont aussi confrontées à ce type de phénomène et se trouvent devant les mêmes problématiques. De plus en plus, les collectivités disposent d'un site Internet où elles valorisent leur attractivité économique et leur potentiel touristique. Certaines mettent en place des actions d'influence[4].

Ainsi les enjeux sont si importants et stratégiques qu'un marché de l'e-réputation a vu le jour en 2006. Certaines agences de communication et de conseil proposent désormais à leurs clients d'examiner leur cyber-réputation et de la corriger si besoin. Des éditeurs de logiciels et agrégateurs issus de l'univers de la veille proposent également des solutions de surveillance de la blogosphère avec différents niveaux de détection de signaux faibles. Des logiciels sont aussi proposés pour gommer les traces sur la toile pouvant devenir préjudiciables. Il existe même aujourd'hui des applications gratuites. Il y a donc des solutions pour tous les types d'entreprises.

Cependant, il ne faudrait pas limiter les enjeux de la réputation numérique à une question de sécurité uniquement et de défense de son image en particulier. En effet, nombre d'entreprises ont compris qu'une bonne gestion de leur identité numérique pouvait constituer un élément de différenciation dans une stratégie de communication. Dès lors, un investissement cohérent de l'espace médiatique que constitue l'Internet d'aujourd'hui peut être un outil de promotion des activités de l'entreprise. Dans cette configuration, des entreprises d'outre-Atlantique n'hésitent pas à recourir à des techniques de narration qui vont scénariser un historique porté par des valeurs positives (*storytelling*). Il s'agit, on l'aura compris, de construire un univers de communication positivé sur l'identité de l'entreprise, destiné à favoriser la vente de produits et services, mais aussi à installer celle-ci dans un rapport de confiance vis-à-vis de ses partenaires.

---

2. http://influx.joueb.com/news/de-l-influence-des-sites-web-sur-les-cours-de-bourse

3. Recommandation N°2002-02 relative à la diffusion d'informations financières sur les forums de discussion et les sites Internet dédiés à l'information ou au conseil financier http://www.amf-france.org/documents/general/3919_1.pdf

4. *Le Dircab guide pratique*, Didier Frochot & Fabrice Molinaro. Territorial Editions. 2009.

C. Les profils (métiers dans l'entreprise) et les secteurs concernés

1. Les services et personnes concernés

Tous les services d'une entreprise sont impactés à des degrés divers. Notons :

La Direction générale et la Direction de la stratégie

Elles ont pour rôle dans ce cas de décider de la stratégie à adopter et de coordonner les différents départements et leur adaptation aux différents canaux en contact avec le monde extérieur en cas d'information négative, de rumeur ou d'action volontairement malveillante.

La Direction de la Communication

Elle a un rôle proactif de surveillance des médias et la charge de diffuser des messages afin de communiquer la position officielle de l'entreprise. Elle doit ensuite veiller à maîtriser ce qui se dit sur l'entreprise. Elle aura enfin la responsabilité de mettre en place des actions correctives suite à une crise afin que l'impact sur l'image de l'entreprise soit le plus minime possible. Elle devra veiller à ce que le message délivré en ligne corresponde au message véhiculé par les services en relation avec les clients.

Le Service de veille ou Intelligence économique

Outre le rôle de surveiller, identifier, analyser et valider les informations, il permet d'apprendre à maîtriser les médias sociaux et d'être davantage préparé à gérer une crise le cas échéant. Pour répondre à des menaces sur l'e-réputation d'une organisation, il est indispensable d'organiser une veille quotidienne du Web. Ce service peut être rattaché à la Direction de la Communication et peut comporter une cellule de gestion de crise.

Le Service juridique

Le droit ne distingue pas les supports de l'information. La liberté d'expression est un principe constitutionnel fondamental et intangible (en France) et globalement cela vaut pour un grand nombre de pays démocratiques. La seule limite au droit d'expression est l'empiètement sur d'autres droits tels la propriété intellectuelle, les atteintes à la personne (respect de la vie privée, diffamation) et plus généralement toutes les atteintes aux droits d'autrui. Le service juridique dispose donc de plusieurs armes.

- Les armes juridiques pour contester sur la forme : le droit de réponse. Depuis la loi du 21 juin 2004 sur la confiance dans l'économie numérique (art 6), les personnes morales ou physiques atteintes peuvent exercer leur droit de réponse : la loi n'impose pas qu'il doit faire suite à des propos négatifs. Cependant ce droit de réponse est rarement employé car c'est une arme à double tranchant à manier avec prudence. Cet article 6 fait aussi référence à la responsabilité éditoriale sur l'Internet qui peut donner des éléments

constituant des armes de défense (responsabilité des hébergeurs, question des liens hypertextes, contrôle des données personnelles…).

- Les armes juridiques sur le fond : la diffamation ou les injures (art 29 de la loi de juillet 1881 sur la liberté de la presse). C'est un terrain d'action sujet à l'interprétation du juge qui doit être pris avec précaution car le risque de perdre un procès peut aggraver une image déjà dégradée. La diffamation ne vise que les personnes physiques ou morales.

Cependant l'une des grandes faiblesses de ces armes est le délai de prescription de 3 mois seulement, qui laisse peu de temps pour identifier la source des propos diffamants et agir en conséquence.

Le Service marketing

En partenariat avec les 2 services suivants et la communication, il est garant de la stratégie produit de l'entreprise. Il veille sur l'environnement concurrentiel de celle-ci et remonte ce faisant des informations de nature à révéler une attaque en provenance d'un concurrent, des griefs de consommateurs, *etc.* Au final, il organise la réplique avec la communication.

Le Service relation clients

Il est en lien avec la communication et doit être en mesure de répondre aux attaques et propos de défiance du consommateur.

Le Service commercial

Il est en contact avec les clients et les fournisseurs en direct pour répondre aux remarques. Les commerciaux sont les premiers à l'écoute de la méfiance et des répercussions d'une mauvaise image, et il est très difficile de vendre des produits et services dans un contexte d'image dégradée. Les répercussions vont donc bien au-delà de la simple baisse des ventes mais peuvent entraîner une baisse de la motivation des personnels concernés et donc de la productivité.

La Direction des ressources humaines et la Communication interne

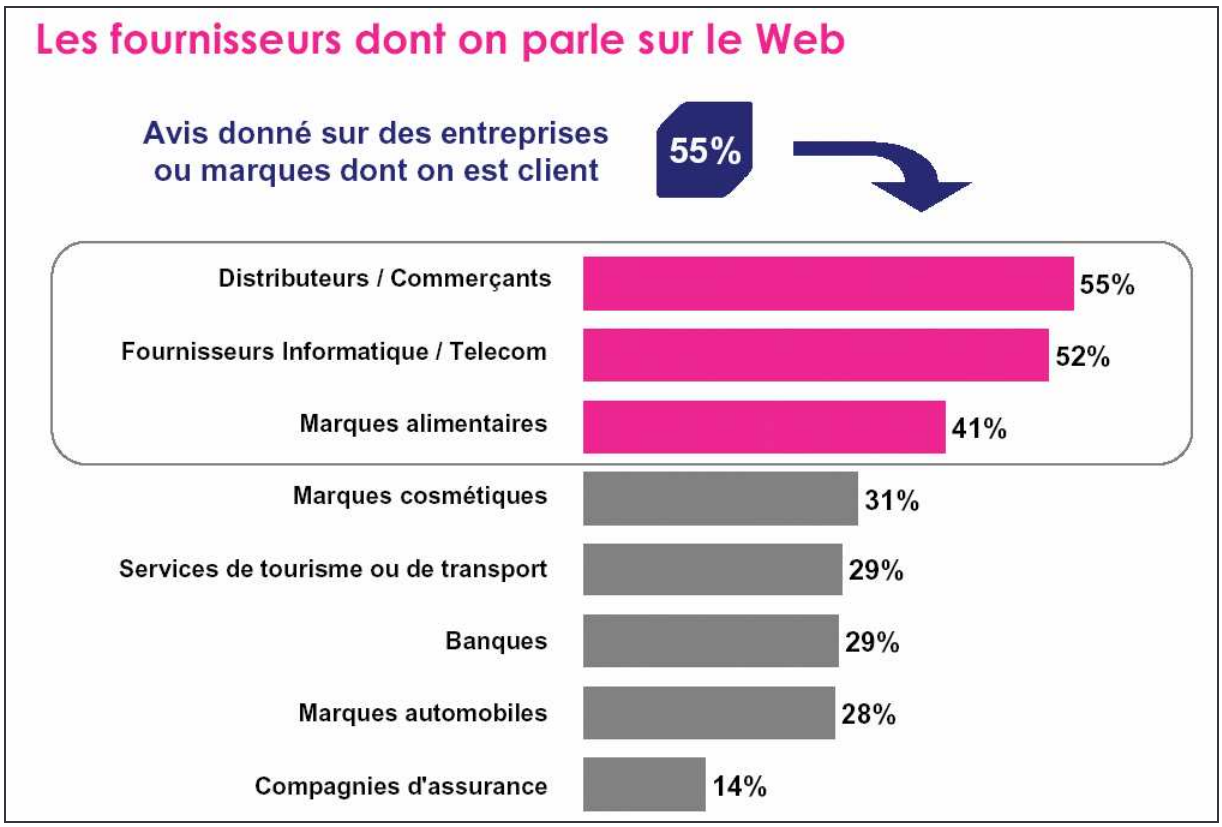
Elles ont pour responsabilité la diffusion de l'information à l'intérieur de l'entreprise. Leur rôle est de s'assurer que chacun connaît les consignes de communication vis-à-vis de l'extérieur : une charte de conduite sur le net peut être rédigée et annexée au contrat de travail, dans certains cas. Ces départements doivent également rassurer les employés et veiller à ce que des éventuelles rumeurs ou attaques n'entravent pas la bonne marche de l'entreprise. Elles veillent à la cohérence interne afin d'éviter toute déstabilisation des effectifs.

2. Les secteurs concernés par l'e-réputation

Si potentiellement tous les secteurs peuvent être concernés, les secteurs s'adressant au grand public et/ou produisant des biens ou services sont soumis à de larges commentaires sur le Web. C'est donc particulièrement le cas pour les produits de grande consommation : high tech, alimentaire, cosmétiques, voyage, tourisme, …

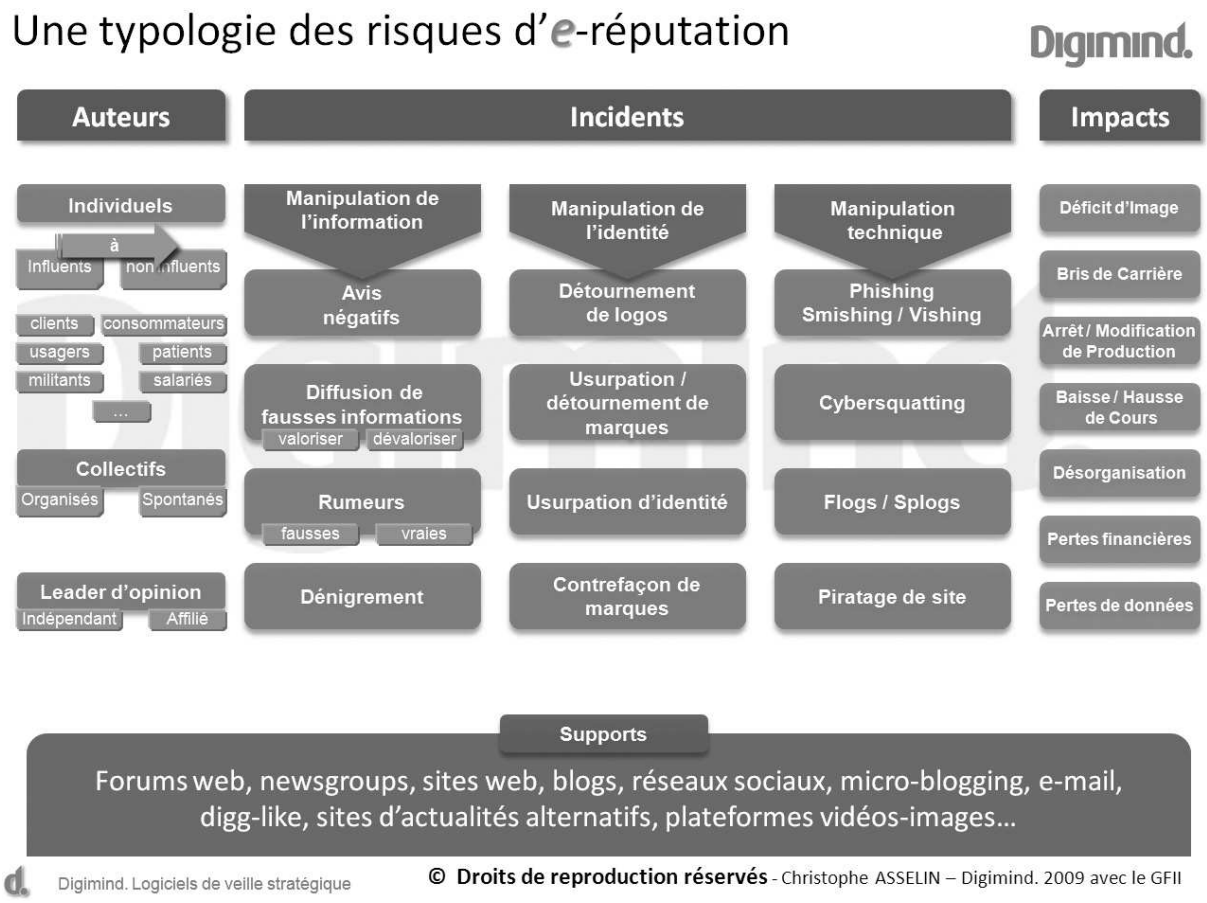
En effet, de plus en plus de consommateurs se basent sur les avis des autres utilisateurs pour se faire une opinion avant un achat. Le discours de l'entreprise devient donc secondaire dans certains domaines et c'est le réseau de pairs qui détient la crédibilité la plus importante.

Les entreprises cotées en bourse ont également une plus grande sensibilité à ce type de menace car elles sont très vulnérables face à des rumeurs dont les conséquences financières peuvent être importantes.



Source : Etude TNS Sofres janvier 2008 : " Web 2.0 : de nouvelles frontières pour la communication corporate ?"

II. Typologie des risques et modes de traitement



A. Avis négatifs d'opinion de consommateurs sur blogs et forums

Une étude publiée sur le blog nord américain 97thFloor[5] a montré que sur les 100 entreprises du classement Fortune 100, 29 étaient dotées de résultats au contenu "négatif" dès la première page de Google, lorsque l'on tape leur nom sur le moteur. Résultats négatifs, c'est-à-dire retranscription de décisions de justices défavorables à l'entreprise ou à sa marque, campagnes de dénigrements, textes de sites contestataires ou commentaires acerbes de clients ou (ex)salariés mécontents.

Description de l'incident

Les avis négatifs émis par des utilisateurs ou par des consommateurs sur un produit, un service ou une société constituent aujourd'hui une part importante de l'image de marque d'une entreprise.

[5] http://www.97thfloor.com/blog/29-fortune-100s-are-letting-google-tarnish-their-reputation/

Si auparavant, hors choc exogène, l'entreprise parvenait à maîtriser assez bien son image avec une stratégie de relations publiques et relations presse, c'est désormais la multiplication des supports de communication qui rend cette stratégie de gestion de la réputation pluri-média plus complexe.

On peut distinguer aujourd'hui plusieurs lieux où les utilisateurs peuvent exprimer leur mécontentement, que l'on peut classer suivant un niveau de risque croissant :

- Les blogs individuels non spécialisés et à faible audience,
- Les blogs individuels non spécialisés et à forte audience,
- Les blogs individuels spécialisés sur l'univers de la marque ou du produit à faible audience,
- Les blogs individuels spécialisés sur l'univers de la marque ou du produit à forte audience,
- Les sites de presse en ligne qui de plus en plus ouvrent des espaces de commentaires,
- Les réseaux sociaux,
- Les forums généralistes,
- Les forums spécialisés,
- Les sites d'avis de consommateurs,
- Les sites d'avis de consommateurs spécialisés (par exemple sur les voyages, les restaurants…),
- Les sites des cyber-marchands.

Plusieurs constats peuvent être dressés :

- N'importe quel message négatif à l'encontre d'une entreprise peut provoquer une réaction en chaîne. Il est difficile de dégager des règles absolues et d'être sûr qu'un message ne se propagera pas.
- Le risque est plus important si :
    - le support sur lequel il est diffusé a une forte audience ;
    - l'audience du site est principalement constituée de clients, de clients potentiels ou de clients correspondant à la cible de l'entreprise ;
    - l'audience du site est constituée de personnes du type « digital natives », maîtrisant parfaitement les réseaux sociaux et le Web 2.0 et ayant pour habitude de publier régulièrement sur Internet.
- La façon dont le contenu est rédigé a une importance forte : plus le discours est posé, argumenté, étayé de faits concrets voire de preuves plus le risque de préjudice est élevé.

Services internes à mobiliser :

- Service Veille qui identifiera le contenu et pourra potentiellement faire un signalement pour contenu ne respectant pas les Conditions Générales d'Utilisation ou pour propos diffamatoires
- Service Communication pour répondre aux propos tenus via les espaces dédiés à cet effet : commentaires / mail de l'auteur…
- Service Gestion de la Relation Clientèle pour entrer en contact direct avec le client et lui faire des propositions concrètes
- Service Juridique en cas de propos diffamatoires ou relevant du traitement juridique (fuites d'informations internes par exemple).

Modes de traitements

Les modes de traitement principaux de ces types de problèmes concernent les sphères « communication » et « juridique ».

Dans le cadre de la communication, les entreprises recrutent de plus en plus de « community managers » qui sont en charge de l'animation des communautés Internet, positives ou négatives, qui se créent autour de la marque. Ce poste peut être assimilé avec celui d'attaché de presse mais son domaine d'action porte sur Internet et particulièrement sur les contenus *UGC*.

Le recours au juridique doit se faire de façon raisonnable et doit rester exceptionnel. Il peut envenimer rapidement une situation si l'arbitrage juridique n'est pas favorable à l'entreprise.

1. Avis individuels

Description de l'incident

Un individu exprime sur Internet un avis négatif sur une personne, un produit, une entreprise. Cet avis négatif, bien qu'individuel, aura un impact plus ou mois fort selon son mode de diffusion. Plusieurs critères sont à prendre en compte :

- la maîtrise des outils par l'internaute : cet avis (article, billet, vidéo, images) pourra être relayé sur plusieurs supports : blogs, réseaux sociaux, site de diffusion de Power Point ou de vidéos…
- la popularité et l'influence de l'internaute : si l'internaute est connu, qu'il est souvent lu, surtout souvent cité et repris dans d'autres médias (pure players Web, presse Web ou presse traditionnelle), son avis aura plus d'impact que celui d'un adolescent qui s'exprime sur un blog lu uniquement par ses amis. Le réseau de l'internaute est également un facteur important : un contributeur qui appartient à une corporation influente (journaliste ou universitaire par exemple) bénéficiera de plus d'amplification.
- Le statut de l'internaute : s'exprime-t-il en toute indépendance ou relaie t-il l'avis (volontairement ou non) d'une entreprise, d'un syndicat ? Ainsi un salarié d'une multinationale dénigrant un concurrent ne pourra pas être considéré de la même manière qu'un internaute isolé : le salarié aura certainement plus de poids dans ses arguments, peut-être aussi plus de moyens pour se défendre s'il blogue officiellement pour son entreprise.

Modes de traitement

Anticipation : il convient, comme souvent en matière d'e-réputation, de savoir et pouvoir anticiper des avis négatifs. Il faut pour cela utiliser des outils de surveillance des concurrents et de toutes organisations ou individus susceptibles de s'exprimer sur un produit ou une entreprise.

Détection : si l'entreprise détecte un message négatif, il convient de « dessiner » le profil de l'auteur pour imaginer des mesures de « correction » adaptées. Comme évoqué plus haut, un journaliste ne peut être contacté de la même manière qu'un adolescent isolé.

Explication : le contact par téléphone est l'idéal, sinon par mail. Il s'agit avant tout de comprendre l'avis de l'auteur et de dialoguer afin d'imaginer avec lui, les solutions possibles. Exemple : une

multinationale attaquée sur ses produits pour animaux dans un forum a contacté 4 contributeurs : ils ont expliqué les raisons de leur mécontentement. L'entreprise a ainsi pu construire une réponse adaptée, publiée sur son site corporate et sur le forum en question.

Procédure : le recours aux services juridiques ne doit intervenir qu'en dernier ressort. Une telle intervention peut en effet faire plus de mal que de bien pour l'entreprise : un blogueur contacté par un avocat aura tendance à évoquer ce type de « pression » sur son blog, attirant davantage de lecteurs et amplifiant davantage son message et sa visibilité. Ces mesures sont donc à proscrire qui plus est dans le cas d'internautes peu influents.

Fiche de relevé d'incident

Avis négatif d'opinion de consommateurs sur blogs et forums
Avis individuel

Profil de l'organisation
Secteur : Banque de détail
Couverture géographique : Implantation nationale

Nature de l'incident/de la menace
Avis négatif sur un blog et des forums
Année de l'incident : 2006

Description de l'incident
En mars 2006, un blogueur révèle qu'un ami homosexuel s'est vu refuser la collaboration d'une banque pour son site de BD gay. Il souhaitait mettre en place un service de transaction électronique.
Motif du refus : la banque ne s'associe qu'à des sites marchands qui proposent des produits "familiaux".
Le client répond que des sites pornographiques hétérosexuels bénéficient du service de paiement électronique.
Les responsables de la banque nuancent leurs précédents propos en annonçant que leur décision n'était pas encore prise définitivement… puisque les sites non conformes à leur éthique devaient être hors zone de la banque.
L'affaire se propage : le blog est assez lu, aussi l'exemple de cette banque est souvent repris.
En tapant le nom de la banque sur Google, vous accédiez dans les premières pages à ce billet de blog (2006) intitulé "La Banque xxxxxxx homophobe"
15 jours plus tard, en avril, la requête de l'ami gay a été honorée par la Banque. La banque lui demande que les billets sur le sujet soient effacés des résultats proposés par les moteurs de recherche, car ils étaient placés en tête des résultats

Services internes à mobiliser : le service de Veille, le Service communication

Modes de traitement
- Technique : mettre en place une surveillance des blogs par le service de veille. S'il est difficile d'analyser les citations sur tous les blogs (une surveillance totale est toujours possible), il est souvent nécessaire, pour cibler sa surveillance, de ne sélectionner que les blogs et sites les plus influents et de n'être alerté que si il y a apparition de certains mots, à certaines fréquences, sur certaines sources seulement.
- Communication : contacter le blogueur directement pour dialoguer avec lui.
- Juridique : A proscrire. Avoir recours au service juridique ou à un avocat pour faire retirer le billet incriminé présente de grands risques : le blogueur peut signaler dans un autre billet, ce qui entraîne souvent un "effet boule de neige". La contrainte d'une autorité fait une grande publicité et augmente la visibilité du blogueur via des titres comme : "Censure de mon blog", "Contrainte de la banque"…

2. Avis collectifs (Associations, lobbies, *etc.*)

Description de l'incident

L'identité numérique peut être malmenée par des groupes de consommateurs organisés ou non.

Une entreprise, un parti politique qui lance un concept, un produit, un service qui déplaît aux clients ou militants peut être rapidement la cible de groupes plus ou moins importants d'internautes critiques.

Ces groupes vont faire pression sur l'organisme à travers des contributions sur Internet. Ces contributions peuvent être de nature très diverses : contestations, appels au boycott, à la désobéissance civile, critiques, plaintes, enquêtes et dossiers parfois très argumentés. Les médias et formats employés peuvent également relever d'une palette très large : billets dans des blogs et des forums, vidéos et images de propagande ou de parodie, détournements graphiques, constitutions de groupes communautaires sur les réseaux de type Facebook ou Twitter, création de sites associatifs sur le Web.

Il faut distinguer 2 grands types de groupes de pressions :

- ceux qui sont déjà structurés et organisés comme une association (qui existe déjà dans le « monde réel » ou qui se crée sur Internet) avec des objectifs et un programme bien défini. Ils interviennent alors au cas par cas sur le net pour mettre en cause une entreprise ou un individu. Exemple : une ONG qui publie un rapport sur Internet pour mettre en cause une multinationale.
- Ceux qui se constituent spontanément à l'occasion d'une crise : par exemple, des consommateurs mécontents d'un service client, d'un fournisseur Internet, vont partager leurs expériences sur un forum, créer un groupe de contestation sur Facebook ou un blog dédié. Ce type de collectifs peut prendre la forme d'un groupe où l'échange entre les membres est une réalité, à l'instar d'une association traditionnelle. A l'opposé, des actions collectives sur Internet ne peuvent être aussi que la somme d'initiatives individuelles, mettant en œuvre des individus qui poursuivent un même but, mais sans interaction et dans une approche purement intéressée. Exemple : des centaines de critiques sur Internet au sujet d'un site de parti politique jugé inepte.

Modes de traitement

- Communication externe : dialoguer d'abord avec les leaders d'opinion du Web, ou les leaders de l'association/lobby. Privilégier une communication orale (téléphone). En effet, des mails pourraient être reproduits par les internautes sur leur blog et être présentés comme des tentatives de pression. Comprendre le point de vue de ces leaders puis expliquer la réponse de l'organisation. Communiquer auprès des journalistes.

- Suivi : réaliser un suivi des publications « correctives » de ces leaders d'opinions pour s'assurer que le message est bien compris. Ex : tel blog très lu a-t-il bien relayé le point de vue de l'entreprise. Poursuivre le suivi des autres supports non leaders pour déterminer si le ou les leaders d'opinion sont bien repris.

- Communication interne : briefer les services en relation directe ou indirecte avec les clients : que doivent-ils répondre aux consommateurs inquiets des informations diffusées sur le Web par un groupe. Les réponses doivent être identiques et homogènes pour tous les services, qui plus est au sein d'un grand groupe. Le type de réponses fournies par un service Client doit être analogue aux réponses diffusées sur le Web. Des réponses divergentes risqueraient d'alimenter une nouvelle crise.

Fiche de relevé d'incident

Avis négatif d'opinion de consommateurs sur blogs et forums
Avis collectif

Profil de l'organisation
Secteur : Opérateur Télécom
Couverture géographique : Implantation internationale

Nature de l'incident/de la menace
Avis négatif sur un blog
Année de l'incident : 2008

Description de l'incident
Une controverse sur les débits d'un smartphone.
En juillet 2008, des discussions apparaissent sur les forums d'un site dédié : un opérateur mobile aurait bridé le débit 3G+ sur le nouveau smartphone afin de ménager sa bande passante : de 380 à 500 kbps attribué à chacun de ses clients, alors que le débit théorique permis par la 3G+ pourrait être de 14 400 kbps.
La "crise" est ensuite relayée sur des blogs de leaders d'opinion high-tech, dans les sites de presse informatique puis dans d'autres forums Web.

Services internes à mobiliser : le service de Veille, marketing, le service Communication, le service Relation Consommateur, la Direction de la stratégie.

Modes de traitement
- Technique : mettre en place une surveillance des blogs par le service de veille afin d'anticiper à l'avenir ce genre de plaintes avant une propagation à un trop grand nombre de sites et de surveiller les réactions aux actions correctives entreprises par le service de Communication.
- Communication : après des dialogues avec les leaders d'opinons Web, et une augmentation du débit, l'opérateur mobile parviendra à apaiser le mécontentement, même si les traces de la controverse sont toujours présentes sur le Web.
- Relation Client : préparer un argumentaire pour les appels des mécontents ayant lu les blogs et sites mettant en cause le bridage de l'opérateur. "L'opérateur est au courant, il va augmenter les débits."
- Juridique : toujours à proscrire. Spécialement dans ce cas où des blogueurs et des sites influents lus relaient l'affaire.

3. Avis d'un leader d'opinion

Description de l'incident

Le concept de leader d'opinion est né bien avant l'essor d'Internet. Dès 1944 Paul Lazarsfeld[6] fait émerger ce concept en publiant une étude sur les motivations des électeurs lors des élections présidentielles américaines de 1940. Un leader d'opinion peut se définir comme un individu qui, par sa notoriété, son titre, son expertise ou son activité sociale intensive est susceptible d'influencer les actions ou les opinions d'un grand nombre d'individus.

Les leaders d'opinion ont trouvé avec Internet un média leur permettant de diffuser facilement leurs idées tout en provoquant des réactions, débats et discussions autour de leurs déclarations. Internet a même favorisé l'essor de nouveaux leaders d'opinions qui n'existaient pas auparavant. Ainsi certaines personnes ont acquis une visibilité grâce aux forums et blogs, à tel point que certains blogueurs sont devenus aussi célèbres que des journalistes TV.

Le leader d'opinion représente une menace pour une entreprise, une marque, dès lors que les internautes adoptent un comportement similaire au sien. Il suffit que celui-ci ait dit du mal d'un produit, déconseillé son usage, voire appelé au boycott, et que les internautes respectent ses recommandations pour que l'impact sur le produit se fasse ressentir. Dans les cas les plus graves, cela peut aller jusqu'à l'effondrement des ventes et du cours de bourse.

Modes de traitement

Anticiper : la maîtrise de son image numérique passe d'abord par l'identification des leaders d'opinion ayant une influence sur son domaine d'activité. L'établissement de cette cartographie permettra de mener, en amont, des actions spécifiques envers ces personnes afin de les rallier à notre cause. Par exemple, ils peuvent faire partie des beta-testeurs avant lancement d'un produit : la démarche a des chances de les séduire, surtout si leurs remarques sont prises en compte dans l'amélioration du produit avant le lancement commercial. Il est même possible d'aller un peu plus loin en offrant aux leaders d'opinion certains avantages, ou certains cadeaux en échange de « services » : inscrire ses « amis » à la newsletter d'une marque, rédaction d'articles sponsorisés, *etc.* Il faut toutefois manipuler tout ceci avec précaution afin que cette stratégie ne se retourne pas contre soi en cas d'insatisfaction du leader d'opinion.

Détecter : il faut également scruter en permanence Internet afin d'identifier l'apparition de toute nouvelle personne influente sur le domaine qui nous intéresse. Cela permettra aussi d'effectuer une veille sur les leaders d'opinion déjà connus afin de détecter les changements de discours et l'émergence de nouvelles problématiques

Experts maison : le leader d'opinion disposant d'un grand capital confiance auprès de sa communauté, il est parfois bon de faire intervenir un expert de la marque dans une discussion. En

[6] ***The people's choice: How the voter makes up his mind in a presidential campaign (1944)***

cas de dénigrement injustifié d'un produit de la part d'un leader d'opinion, l'expert viendra apporter des arguments tangibles qui ne pourront pas être démontés et qui provoqueront une perte de crédibilité du leader d'opinion.

Offrir un espace d'expression : il est également possible de faciliter le contrôle des commentaires en créant un espace d'expression libre sur lequel tout internaute (leader d'opinion y compris) pourra laisser des messages. Cela peut prendre la forme d'un blog d'entreprise ou d'un forum par exemple. Cet outil a le double avantage de faciliter la mesure de la satisfaction de l'opinion à l'égard d'une nouvelle offre et de permettre une réaction immédiate lorsqu'il est nécessaire de rétablir la vérité ou de modérer les échanges.

Fiche de relevé d'incident

Avis d'un leader d'opinion

Profil de l'organisation

Secteur : Constructeur informatique

Effectif : plus de 75 000

Couverture géographique : Présence internationale

Nature de l'incident/de la menace

Un journaliste connu fait état sur son blog des problèmes qu'il rencontre avec l'ordinateur dont il vient de faire l'acquisition et avec le SAV du constructeur.

Année de l'incident : 2005

Exposé de l'incident

Un journaliste américain connu, blogueur assidu, rencontre de nombreux problèmes avec l'ordinateur qu'il vient d'acquérir auprès d'une marque célèbre. Non seulement, le matériel ne fonctionne pas, mais l'extension de garantie avec intervention à domicile qu'il a souscrite ne peut pas être mise en œuvre dans le cadre de son problème. Mécontent, il décide de publier sur son blog un journal de ses mésaventures. Un véritable buzz naît : des centaines d'autres blogueurs réagissent et publient leurs propres déboires avec la marque. La presse écrite s'empare du sujet et rédige de pleines pages sur cette affaire, les ventes du constructeur s'effondrent et le cours de bourse s'écroule.

L'affaire est ponctuée par une lettre ouverte du journaliste à l'intention du PDG de la marque dans laquelle il lui communique quelques conseils sur le bon usage qu'il pourrait faire des blogs.

Modes de traitement

Services internes ayant été mobilisés : Direction Générale, Communication, Service Clients

Mode de traitement : la première réaction du constructeur fut de fermer les forums communautaires disponibles sur son site. Cela n'eut pour effet que de renforcer la vigueur des critiques sur la qualité du service client.

Finalement, le constructeur finit par comprendre l'intérêt d'une proximité et d'un dialogue avec ses clients et ouvre un wiki et un blog d'entreprise.

B. Diffusion de fausses informations

Description de l'incident

La diffusion d'une fausse information sur Internet consiste à communiquer des données erronées ou déformées sur un individu, une organisation, un pays afin de modifier leur perception auprès du public. Cette action peut être réfléchie ou non, individuelle ou collective. Un individu isolé peut ainsi dénigrer une entreprise et ses résultats économiques dans le but de faire baisser le cours de ses actions.

A l'inverse, il est possible de diffuser de fausses informations très positives au sujet d'un individu ou d'une organisation afin d'augmenter artificiellement la valeur de celle-ci. Une entreprise qui propage de fausses informations sur l'ouverture prochaine d'usines ou la sortie de nouveaux produits peut ainsi attirer des investisseurs ou des médias.

La diffusion de fausse information est un processus volontaire destiné à nuire ou à enjoliver la réalité. Elle diffère en cela des processus de rumeurs classiques où le cheminement et les cibles sont rarement anticipés et définis en amont. La déstabilisation sur Internet est une conséquence fréquente de la diffusion de fausse information.

Modes de traitement

La rapidité de réaction est le critère essentiel pour réagir à la diffusion de fausses informations

Il faut pour cela disposer :

- d'outils permettant la surveillance d'un spectre très large de sources d'informations sur Internet ne se limitant pas aux sites Web classiques ;

- d'une organisation interne souple permettant une bonne réactivité : des outils de détection puissants ne servent à rien si le service de communication (par exemple) ne rédige pas dans des délais courts un contre-communiqué ;

- d'une équipe aguerrie à la construction de contre-communiqués ou à l'intelligence économique défensive : il s'agit d'argumenter avec le plus de conviction (et de talent) possible afin de prouver de manière irréfutable que l'information est fausse. Des approximations de termes ou des arguments peu convaincants pourraient produire l'effet contraire : la naissance d'une rumeur. (par exemple, une entreprise de vente par correspondance explique une erreur de prix d'affichage, mais avec trop de retard et de manière trop brève. Nombre d'internautes n'y croient pas et contribuent à lancer une rumeur sur l'incompétence de l'entreprise).

On veillera particulièrement à utiliser le maximum de canaux de communication (presse, Web) et à privilégier les médias qui touchent les cibles les plus concernées par la diffusion de la fausse information. Ainsi, un communiqué de presse se limitant aux sites Web classiques ne touchera pas des cibles d'adolescents plus présents sur les réseaux sociaux.

Le service juridique assisté du service d'intelligence économique devra ensuite s'employer à identifier la personne à l'origine de la diffusion de la fausse information. Ce type d'action doit s'effectuer en toute confidentialité afin de ne pas transpirer sur le net : un buzz autour de la recherche de « coupable » nuit à la réputation d'une entreprise.

Fiche de relevé d'incident

Diffusion de fausse information

Profil de l'organisation
Secteur : Transports et entreposage
Effectif : Plus de 1000 salariés

Couverture géographique : Implantation physique nationale et européenne

Nature de l'incident/de la menace
Diffusion de fausses informations
Diffamation
Communication de documents et renseignements d'ordre économique et commercial
Année de l'incident : 2005

Exposé de l'incident
Une rumeur diffusée massivement sur Internet via les blogs, les forums, les associations de consommateurs, les syndicats et reprise rapidement par la presse généraliste, a fortement nuit à l'image de cette entreprise sans que cette dernière ait pu contrôler la diffusion de l'information diffamatoire.

Services internes ayant été mobilisés : Communication, Sûreté, Ressources Humaines

Modes de traitement : Communication

Procédure : Démenti publié dans la presse après l'incident, notamment sur le site http://www.hoaxbuster.com/
Recours à des prestataires extérieurs privés : éditeur de logiciel de veille sur Internet fournissant également un accompagnement à ses clients.
Pas de recours à une administration ou autorité publique

Résultats
Délai entre le constat et la résolution : la résolution du problème s'est faite avec la mise en place de la cellule de veille, soit environ 1 mois. Les autres problèmes ont été gérés en moins de 48h avec une cellule de crise.
Identification de l'origine – mode d'identification de l'origine :
Le problème a été identifié grâce à une cartographie du Web et de la blogosphère. Une fois les relais d'influence détectés, le mode opératoire consiste à la prise de contact directe avec les auteurs des blogs, sites Web ou autres modérateurs de forums.
Mesures prises à l'issue de cet incident :
Contrôle systématique des informations diffusées sur Internet concernant l'entreprise.
L'entreprise peut également utiliser cette solution pour anticiper les rumeurs, mettre en place des plans de communications adéquats, publier des communiqués avant que les rumeurs ne soient massivement diffusées sur le Web.
Ceci permet également à l'entreprise de communiquer en interne de façon plus proactive avec ses salariés.

Fiche de relevé d'incident

Déstabilisation sur Internet via de fausses informations

Profil de l'organisation
Secteur : Constructeur informatique
Couverture géographique : Implantation internationale

Nature de l'incident/de la menace
Diffusion de fausses informations
Année de l'incident : 2007

Description de l'incident
Chute des cours d'un constructeur informatique :
16 mai 2007, 11H49 : le site/blog américain Engadget, annonce que, selon un mémo interne transmis par un employé d'un grand constructeur informatique, la prochaine version du système d'exploitation et son nouveau téléphone seraient retardés de plusieurs mois. Engadget est très suivi par les investisseurs américains.
Quelques minutes plus tard, le cours de l'action du constructeur chute de 107,89 à 104,63 $. Vers 12h15, Engadget corrige son article : le mémo était un faux. La prochaine version du système d'exploitation et le nouveau téléphone ne seront pas en retard. Le cours de l'action remonte sur 107.30 mais ne retrouve pas sa valeur d'ouverture (107.55).

Services internes à mobiliser : le service de Communication, le service de veille, le service Intelligence Economique défensif, Sécurité, Juridique

Modes de traitement
- Communication : grâce à une surveillance des sites de presses et des blogs en temps réel, le constructeur peut réagir en 10 minutes et contacter le blog qui a publié l'information pour lui signaler que l'information est fausse.
- Il faut ensuite publier un communiqué de démenti très rapidement et l'envoyer à la presse mais aussi aux blogueurs les plus influents.
- Intelligence Economique défensive : tenter de trouver l'origine de la désinformation : origine interne, origine extérieure avec volonté de nuisance manifeste.
- Juridique : s'il s'avère que la désinformation est une tentative délibérée pour nuire à la réputation de l'entreprise voire manipuler les cours de bourse, une action pour diffamation est possible.

C. Rumeur sur Internet

Description de l'incident

La rumeur sur Internet est une transposition sur le réseau numérique de la rumeur hors média : la structure du réseau Internet et la multiplication des réseaux sociaux permettent beaucoup plus facilement qu'hors-ligne la propagation d'une rumeur. La transmission s'effectue dans une forme stable autorisant rarement des tournures plus nuancées ou bien sa rapide disparition.

La rumeur peut être négative ou positive et dans un cas comme dans l'autre, fondée ou infondée. On parlera de rumeur lorsque sa source ne peut être clairement être identifiée ou que le processus de création de cette information n'est pas clairement identifiable. Dans le cas où elle est orchestrée et négative, la rumeur relève d'une manœuvre de déstabilisation.

La rumeur est d'autant plus difficile à gérer et à endiguer qu'elle va reposer sur des faits pour lesquels il sera difficile d'apporter une preuve les démentant. Par ailleurs, la rumeur n'est pas forcément ciblée contre une entreprise en particulier. Reposant souvent sur des « peurs personnelles » celle-ci peut impacter directement l'activité d'une entreprise, le rappel de cette peur étant un frein à l'achat.

On pourra prendre comme exemple de cas de rumeur, celui relatif aux dangers liés à l'absorption de Vodka Red Bull pouvant aller jusqu'à provoquer la mort[7].

Services internes à mobiliser

- Service veille : il joue un rôle prépondérant dans la résolution des problèmes liés à la rumeur en permettant l'identification rapide et donc une action avant que sa diffusion ne soit excessive.
- Service communication : la prise de parole rapide et transparente de l'entreprise concernée est essentielle.

Modes de traitement

C'est la communication qui joue un rôle essentiel dans le traitement de ces crises liées à la rumeur. Plus cette communication est réactive, plus celle-ci a une chance d'être endiguée.

La communication devra se faire de façon argumentée, et reposer sur des faits concrets afin de s'opposer par le ton adopté au catastrophisme ou aux exagérations.

On privilégiera les réseaux officiels et médias traditionnels afin d'apporter un crédit supplémentaire au message diffusé par l'entreprise.

Les médias alternatifs, blogs, forums et autres ne devront pas être ignorés afin de toucher et convaincre les internautes souvent véhicules de la rumeur.

[7] http://www.hoaxbuster.com/hoaxliste/hoax.php?idArticle=77986

On prendra soin de faire figurer la rumeur en question sur les sites de référence listant les différentes rumeurs (par exemple pour la France, www.hoaxbuster.com).

Si bien souvent la rumeur issue d'une information véridique s'éteint d'elle-même, la rumeur construite à partir de fausses informations est beaucoup plus complexe à maîtriser et à éliminer de la pensée collective. Plus une rumeur fausse apparaît comme crédible, plus elle sera difficile à endiguer. Mais les critères renforçant une fausse rumeur ne se limitent pas à son caractère probable. Une rumeur, montée de toute pièce, peut bénéficier d'une amplification importante si :

- elle fait appel à des peurs collectives (la crainte de l'étranger pour la rumeur d'Orléans) ;

- elle repose sur des schémas de pensée fortement ancrés (méfiance de la province envers Paris lors des rumeurs d'inondations de la Somme) ;

- elle recycle des légendes urbaines qui ont déjà fonctionné (des seringues infectées du sida dans les sièges d'un cinéma) ;

- elle cible un organisme ou une personnalité (Dominique Baudis et l'affaire Patrice Alègre).

Fiche de relevé d'incident

Rumeur sur Internet

Description de l'incident

Le buzz sur un médicament : à qui profite la rumeur ?

Un médicament d'un laboratoire pharmaceutique est indiqué pour le sevrage tabagique (promesse d'arrêt d'envie de fumer) chez l'adulte. A l'automne 2007, une rumeur s'est propagée aux Etats-Unis.:

3 Septembre 2007, Dallas, Texas : Carter A, un membre d'un groupe de rock local, est mort des suites d'actions violentes et irrationnelles. Un soir, il frappe son amie puis tente de défoncer à coup de pied la porte du voisin de sa compagne. Le voisin effrayé réplique en tirant une balle dans la tête du musicien. L'autopsie révélera un taux d'alcool trois fois supérieur à la limite légale.

La rumeur se diffuse ensuite en plusieurs étapes :

- Carter A avait un comportement agité depuis plusieurs semaines, explique sa petite amie. Il utilisait le médicament pour cesser de fumer.

Le 5 septembre, elle déclare au site de presse texan Dallas News : "Je pense vraiment que c'est à cause du médicament [...]. Il n'avait jamais eu de comportement violent avec moi auparavant. Il était vraiment pacifique". S'en suivent plusieurs articles dans la presse et les sites Web locaux qui évoquent la prise du médicament par le musicien.

Alors que depuis quelques semaines, des utilisateurs du médicament se plaignent sur les blogs de comportements agités et violents, ni la FDA (autorité régulatrice américaine des médicaments), ni le laboratoire pharmaceutique, ni d'autres chercheurs n'ont pu lier la molécule à des comportements violents pour ses effets secondaires. Mais, les parents du musicien expliquent à la presse que son comportement violent ce soir là est dû au médicament. Quoiqu'il en soit, le buzz, qui au départ est faible (quelques dizaines de billets sur les effets secondaires, ce qui est peu pour un médicament blockbuster), commence à s'amplifier à partir de ce fait divers mettant en scène une personnalité locale.

Et rien ne peut enrayer ce buzz : en octobre, le rapport médical final effectué dans le cadre de l'enquête de police a beau révéler l'absence de consommation de drogue y compris le produit incriminé, la famille persiste. Le père du musicien conteste ce rapport, arguant du fait qu'il n'existe aucun test permettant de déceler la présence ou non du médicament anti-tabac.

- A partir de la mi-septembre 2007 et jusqu'en février 2008, 3 types de buzz coexistent sur le Web (blogs, forums et sites d'actualités) :

- les conversations et articles associant la mort du musicien au médicament (volume faible).

Les titres peuvent utiliser des raccourcis sans équivoque, très dommageables pour le laboratoire. Exemple : "*drug Y killed Carter A.* " écrit le blog The Unticket.com.

- les conversations et articles associant le musicien et le médicament mais en ne formalisant pas de lien de cause à effet entre sa mort et les effets secondaires (volume moyen). Exemple : «Seeking to Explain Final Acts of Violence" écrit le New York Times.

- les conversations et articles évoquant les effets secondaires du médicament, dépression, idées suicidaires sans mentionner le musicien texan (volume très important) : "*Scary Side effects of drug Yx*" dans The People's pharmacy.

Services internes à mobiliser

Le service de Communication, le service de veille, le service Intelligence Economique défensif, le service de lobbying.

Modes de traitement

- Communication : démontrer à l'aide de communications auprès de la presse, des sites Web, des praticiens qu'il n'y pas de lien de cause à effet prouvé et avéré entre le décès et la prise du médicament.
- Lobbying : multiplier les entretiens avec les journalistes afin d'occuper l'espace médiatique et de leur prouver la bonne fois du laboratoire.
- Veille : surveiller les réactions de la presse et des blogueurs face aux actions correctives du laboratoire.
- Intelligence Economique défensive : rechercher si des "éléments extérieurs" (laboratoires concurrents) ne sont pas mêlés à l'origine de la rumeur et/ou à sa propagation.

D. Dénigrement sur Internet

Description de l'incident

Le dénigrement consiste à jeter publiquement le discrédit sur une personne ou une entreprise afin de nuire à sa réputation. S'il a toujours existé, l'explosion des nouveaux médias et particulièrement d'Internet, a créé un terreau fertile à la multiplication des actions de dénigrement. Il est intéressant de noter que ces actions peuvent s'appuyer sur des rumeurs, avérées ou non (voir point 2.3 de ce document : « Rumeur sur Internet »). Le dénigrement sur Internet est donc une action ou une série d'action ayant pour but de discréditer une société, une marque, des produits ou une personne sur le Web.

Avec l'émergence du Web 2.0 et la multiplication des contenus générés pas des utilisateurs (*UGC* : *User generated content*), il est facile et rapide de publier de l'information sur Internet. Ceci signifie qu'il est de plus en plus facile de tenter de dénigrer une société ou ses produits sur Internet, avec un anonymat relatif (en tout cas ressenti par la plupart des utilisateurs).

Il est possible de jeter le discrédit sur une société en diffusant de fausses informations sur différents supports (blogs, forums, commentaires de sites d'actualité, réseaux sociaux) ; du fait de la structure du Web, ces informations, si elles ne sont pas détectées ou corrigées à temps par l'entité visée, pourront se diffuser rapidement et largement.

Services Internes à mobiliser

Service veille qui a pour mission d'identifier les sources d'information potentiellement dangereuses en termes de dénigrement (complexe du fait de la disparité de l'information sur le Web) et de surveiller le Web de façon plus générale (méta moteurs, outils de veille automatisée, agrégateurs de flux, réseaux sociaux) afin d'être alerté dès l'apparition d'information évoquant la société (produits, dirigeants, etc.) dans le but de pouvoir réagir rapidement en cas de dénigrement avéré.

Service juridique car le dénigrement constitue une attitude fautive au sens de l'article 1382 du code civil. Il peut aussi être constitutif de concurrence déloyale lorsqu'il consiste à jeter publiquement le discrédit sur les produits ou services d'une entreprise. Le dénigrement pourra être invoqué si toutes les conditions de la diffamation ne sont pas réunies (pas d'imputation d'un fait précis) ou que l'action est prescrite. Le service juridique aura donc la charge de poursuivre en justice les personnes ou organisations à l'origine de l'action de dénigrement, lorsque ceux-ci sont identifiables et identifiés, en fonction du préjudice subi (déficit d'image, concurrence déloyale, perte de marchés, *etc.*).

Service communication qui devra, en fonction des cas :

- Informer le public de la diffamation avérée (en accord avec le service juridique).
- Communiquer sur les médias adaptés (en fonction des supports qui ont véhiculé l'information) avec un discours élaboré en tenant compte des supports.

Modes de traitement

Communication : lorsque le format et le média le permettent (sites de presse, blogs professionnels, etc.) il est souhaitable de solliciter dans un premier temps un droit de réponse en ligne, qui permettra dans certains cas, de diminuer l'impact négatif éventuel d'informations, si celles-ci sont détectées assez en avance.

Juridique : il convient aussi de demander au tribunal de supprimer les messages dénigrants ainsi que d'exiger la publication, sur la page d'accueil du site Web, de la décision de justice, pour une durée déterminée. Il est aussi possible que le tribunal exige une publication de la décision dans un ou plusieurs quotidiens nationaux. Cependant, ces actions peuvent être complexes à mettre en œuvre lorsque les auteurs du site ne sont pas identifiés et/ou que les sites en question sont hébergés à l'étranger.

Fiche de relevé d'incident

Dénigrement sur Internet

Profil de l'organisation
Secteur : Production et distribution d'électricité, de gaz, de vapeur et d'air conditionné
Effectif : Plus de 1 000 salariés
Couverture géographique : Implantation physique internationale

Nature de l'incident/de la menace
Contrefaçon de marque
Dénigrement sur Internet
Diffusion de fausse information
Année de l'incident : 2002

Exposé de l'incident
Une ONG via son site Internet communique sur les actions qu'elle mène à l'encontre de l'entreprise et invite les internautes à signer une pétition contre une partie de l'activité de l'entreprise en reproduisant le logo et le nom de la société associés à une tête de mort et à un slogan très négatif. Les tribunaux ont été saisis.

Services internes ayant été mobilisés : Communication

Modes de traitement : Juridique et Communication
Procédure :
- Acte d'huissier assignant l'association en contrefaçon pour reproduction et par imitation des marques et pour avoir commis des actes fautifs distincts discréditant et dévalorisant l'image des marques litigieuses. Demande de paiement d'une somme 20 000 euros en réparation des actes fautifs.
- Assignation de l'hébergeur du site en jugement commun.
- Recours à des prestataires extérieurs privés : huissier et avocat spécialisé en propriété intellectuelle.
- Recours à une administration ou autorité publique : tribunal de grande instance.

Résultats
Décision du tribunal rendue 24 mois après les premières constatations d'huissiers :
- Déboute la société de son action en contrefaçon des marques.
- Confirme les actes de dénigrement du fait de l'association des images de mort à la reproduction des marques.
- Condamne l'association à arrêter la poursuite de ces agissements et au paiement de dommages et intérêts et autorise la société à faire publier la décision de justice dans trois journaux aux frais de l'association.
- Donne acte à l'hébergeur d'appliquer la décision.

E. Détournement de logo (Logo busting)

Description de l'incident

Le logo est l'une des composantes d'une marque. Associé à une signature, il résume le message que la marque souhaite véhiculer auprès de ses clients : valeurs, personnalité et principaux attributs. En voyant le logo et sa signature, un client peut ainsi se faire rapidement une idée de la promesse à laquelle la marque est associée.

Parfois utilisé en appui d'une action de dénigrement (cf 2.4 ci-dessus), le détournement de logo peut être utilisé par tout internaute qui a le sentiment qu'une marque n'agit pas conformément aux valeurs affichées. Il est alors facile d'insérer le logo et sa signature dans un autre contexte pour leur faire dire autre chose.

Les dégâts sur la marque sont d'autant plus forts si le détournement de logo est associé à un fait d'actualité qui révèle des agissements de la marque inconnus du plus grand nombre et qui s'inscrivent effectivement dans une démarche opposée aux valeurs publiquement affichées par la marque.

Il est évident que l'essor du Web 2.0, qui offre un espace d'expression libre à toute personne qui le souhaite, accentue l'effet dévastateur pour une marque victime de détournement de logo. Tout d'abord il est quasiment possible de tout dire et tout montrer sans aucune censure : l'espace d'expression n'est pas limité (au contraire d'un journal papier ou télévisé) et les messages sont rarement filtrés (au contraire d'un comité de rédaction qui fait des choix éditoriaux par exemple). De plus la propagation du message peut être très forte : les médias participatifs sont reliés les uns aux autres et offrent des espaces de commentaires permettant d'engager des discussions autour d'un sujet.

Les internautes qui souhaitent faire entendre leur voix ont donc tous les outils à portée de clic et toutes les chances d'être entendus.

Modes de traitement

Anticiper : comme on l'a vu, Internet favorise une circulation rapide de l'information ; il faut donc pouvoir agir rapidement et traiter le problème le plus en amont possible. Pour cela, l'entreprise doit effectuer une veille sur ses marques en privilégiant la surveillance de sources dans lesquelles l'incident a le plus de chances d'apparaître : blogs, réseaux sociaux, forums de discussion. La plupart des plateformes logicielles du marché permettent d'effectuer cette surveillance de manière automatisée.

Evaluer l'ampleur de l'impact : l'action corrective doit être adaptée à l'incident. La mise en œuvre de moyens disproportionnés ne ferait que donner une résonnance médiatique à un incident qui aurait pu rester isolé. Ainsi, il est utile de se poser diverses questions avant d'agir : quelle est l'influence du blog ? Quelle est la notoriété de l'auteur du détournement de

logo ? Quelle est la popularité de la source sur laquelle le détournement est publié ? A quelle vitesse se propage l'information ?

Démentir : cet exercice est périlleux et peut, comme précisé plus haut, être plus dévastateur que le détournement de logo lui-même. En portant le débat sur la place publique, on révèle le problème et on n'est pas certain de convaincre l'opinion publique. Tout démenti devra donc être mûrement réfléchi et il est vivement recommandé de se faire assister par des spécialistes en communication de crise avant d'enclencher une telle opération.

Contacter les auteurs du détournement de logo : le détournement de logo peut cacher l'insatisfaction d'un client qui rencontre un problème avec la marque et qui utilise cette manœuvre pour effectuer une pression en vue de la résolution de son problème. Dans un tel cas, il est nécessaire d'engager la discussion avec le client. Le plus souvent la résolution de son problème permet d'obtenir la suppression de la page contenant le logo détourné. Cependant, le logo a pu être détourné pour des raisons plus philosophiques (non adhésion au comportement de la marque, remise en cause des méthodes de management, protestation contre la délocalisation dans des pays où les droits de l'homme sont bafoués, etc.). Dans ce cas, la tentative de négociation avec l'auteur du détournement de logo doit être faite prudemment car en cas de refus la capacité de nuisance de l'auteur pourrait être décuplée.

Poursuivre en justice : là encore, il faut être bien conseillé afin d'engager des poursuites pour les bons motifs. Les attaques en contrefaçon ont en effet très peu de chances d'aboutir dès lors que le but de l'auteur n'était pas de concurrencer l'activité de la marque. En revanche, si le détournement de logo vise à dénigrer la marque, à dire du mal dans l'intention de nuire, alors la marque a plus de chances obtenir la condamnation de l'auteur et la réparation du préjudice.

Fiche de relevé d'incident

Détournement de logo

Profil de l'organisation
Secteur : Fabricant - téléphonie mobile
Effectif : Plus de 125 000 salariés
Couverture géographique : Présence internationale

Nature de l'incident/de la menace
Détournement de logo par des internautes.
Année de l'incident : 2009

Exposé de l'incident
Un fabricant de renommée mondiale lance une campagne de communication visant à faire gagner des bons de réduction pour l'achat de téléphones portables. Seulement quelques jours après le début de la campagne, le Wall Street Journal publie un article dans lequel on apprend que ce fabricant a vendu à un pays du Moyen-Orient une technologie qu'il utiliserait pour espionner les conversations de ses citoyens et débusquer les opposants sur Internet. Informés de cet article, plusieurs internautes vont récupérer le logo de la société accompagné de sa signature et le superposer sur des photos illustrant une répression d'opposants au régime.
Le détournement de logo, d'abord publié sur des blogs, est rapidement repris par d'autres internautes sur d'autres supports. Ainsi, 15 jours après le lancement de la campagne de communication, on ne comptait qu'un seul tweet (message publié sur Twitter) faisant référence à cette campagne. Au même moment, on comptait 3 tweets par heure sur la polémique impliquant le fabricant…

Services internes ayant été mobilisés : communication, veille des médias

Modes de traitement
L'incident est détecté très rapidement par la cellule de veille qui opère une surveillance des médias sociaux. Le service communication diffuse sur le blog détracteur un communiqué officiel démontrant sa non-implication dans l'organisation d'un système d'écoute. En parallèle, l'agence de communication du fabriquant contacte le blog détracteur afin de proposer un partenariat pour faire la promotion de la campagne officielle.

Résultats
L'impact de la première action est malheureusement annihilé par celui de la deuxième. Le fait d'être contacté par l'agence de communication est vécu comme une provocation : l'information est divulguée sur le blog ce qui entraîne une nouvelle vague de commentaires négatifs. Cependant, la polémique n'est finalement que très peu reprise par les médias traditionnels et s'éteint au bout de quelques jours.

F. Usurpation d'identité

Si des cas d'usurpation d'identité de célébrités sont connus, ce risque peut aussi concerner des personnes moins médiatiques. Les objectifs poursuivis dans l'usurpation d'identité sur des réseaux sociaux peuvent être la déstabilisation, en diffusant de fausses informations voire des informations diffamatoires, mais également le renseignement.

Modes de traitement

1. Demande de suppression d'un profil sur un réseau social

Cette démarche est prévue sur tous les réseaux sociaux. Le simple recours à l'administrateur de la plateforme peut être suffisant. Par exemple, il est possible de contacter Facebook pour signaler un faux profil, en envoyant un message à l'adresse privacy@facebook.com et en indiquant de manière précise la partie du profil où la violation des conditions d'utilisation est constatée.

2. Vérification des comptes par les réseaux sociaux

Twitter a lancé à l'été 2009 une version beta d'une technologie de vérification de comptes.

3. Action juridique

En France, l'usurpation d'identité peut être dans certains cas sanctionnée de 5 ans d'emprisonnement et de 75 000 euros d'amende (article 434-23 du Code Pénal) : « le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales, est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende». La qualification d'usurpation d'identité est strictement encadrée par la jurisprudence.

La Loi d'orientation et de programmation pour la performance de la sécurité intérieure, prévoit de modifier l'article 222-16-1 du Code pénal, qui serait ainsi établi :

« Art. 222-16-1. - *Le fait de faire usage, sur un réseau de communications électroniques, de l'identité d'un tiers ou de données de toute nature permettant de l'identifier, en vue de troubler la tranquillité de cette personne ou d'autrui, est puni d'un an d'emprisonnement et de 15 000 € d'amende.*

« Est puni de la même peine le fait de faire usage, sur un réseau de communications électroniques, de l'identité d'un tiers ou de données de toute nature permettant de l'identifier, en vue de porter atteinte à son honneur ou à sa considération. »

Il est également à signaler que la commission européenne a lancé à l'été 2009 un appel d'offre concernant une « **Étude comparative des instruments de prévention et de lutte contre l'usurpation d'identité dans les États membres de l'UE ».**

L'étude devra notamment envisager sur la base des mécanismes de dénonciation identifiés dans les États membres de l'UE, des recommandations sur la façon de promouvoir l'établissement de guichets uniques pour les victimes d'usurpation d'identité au sein de l'Union européenne, sur leur manière d'opérer afin d'être les plus efficaces possible et sur la façon d'encourager les échanges de meilleures pratiques et la coopération entre eux. En se basant sur l'étude, la Commission devra

être en mesure d'évaluer la nécessité de présenter une proposition législative (qui sera sujette à une analyse d'impact ultérieure) et sa valeur ajoutée, et d'harmoniser les dispositions du droit pénal dans l'Union européenne en ce qui concerne l'usurpation d'identité. La Commission devra également être en mesure de promouvoir les meilleures pratiques existantes en matière de mécanismes de dénonciation pour les victimes (par exemple, assistance juridique, partage d'information, statistiques, enquêtes spécifiques sur la persécution, sensibilisation) et évaluer les mérites d'autres initiatives facilitant l'établissement de guichets uniques pour les victimes de l'usurpation d'identité dans l'Union.

Fiche de relevé d'incident

Usurpation d'identité

Profil de l'organisation
Secteur : Humanitaire
Couverture géographique : Implantation physique internationale

Nature de l'incident/de la menace
Usurpation d'identité
Année de l'incident : 2009

Exposé de l'incident
Un cadre d'une entreprise de médias se rend compte, par hasard qu'il y a deux comptes Facebook à son nom, l'un qu'il a créé, l'autre créé par un tiers, qui a redéfini son réseau d'amis. Ce clone est particulièrement bien dessiné puisque le profil dispose de nombreuses photos privées et est actif quotidiennement. Parmi les proches de ce cadre, figure un militant des droits de l'homme, installé dans une dictature militaire. Après une rapide enquête, il semble que cette usurpation d'identité ait permis de surveiller les activités et le réseau de ce proche.

Modes de traitement : Communication
Procédure :
Demande de suppression du profil à Facebook.
Information du réseau concerné sur cette usurpation d'identité.

Résultats
Suppression rapide du profil Facebook.

G. Phishing / Smishing / Vishing

Description de l'incident

Le phishing consiste à tromper un internaute sur l'origine d'un message afin de lui soutirer des informations confidentielles. Cette arnaque s'est beaucoup développée en ciblant les clients des banques en ligne. Elle consiste à faire parvenir un courriel ayant l'apparence habituelle de ceux de la banque demandant une action au client en raison d'un incident quelconque. Le client est invité à saisir des informations confidentielles le concernant. La sophistication peut être importante avec un faux site reprenant sur une ou plusieurs pages tous les attributs du site de la banque. Une version plus simple demande d'envoyer les informations par fax… Les mêmes techniques sont employées pour accéder aux réseaux d'une entreprise et à ses informations sensibles. Les clients des fournisseurs d'accès Internet et des sites de vente en ligne ont également été visés. L'évolution montre toutefois que l'arnaque la plus courante concerne les données de carte bancaire, faciles à utiliser et à monétiser.

Récemment, le phishing s'est également développé auprès des utilisateurs de réseaux sociaux, permettant aux pirates de récupérer des informations confidentielles (et parfois monnayables), ou de faire des dégâts dans la vie privée des personnes.

L'hébergement des faux sites s'est beaucoup sophistiqué : il peut être sur un serveur pirate ou un serveur légitime, sur une seule machine ou sur des centaines en même temps, il peut être indépendant ou venir chercher des ressources sur les sites légitimes.

Le néologisme phishing a été construit à partir des mots phreaking (autre néologisme désignant le piratage téléphonique) et fishing (pêche). En français, hameçonnage est parfois utilisé pour désigner le phishing.

La technique de phishing s'est récemment étendue aux terminaux mobiles. Cette version appelée smishing (lire SMiSing) consiste à piéger l'utilisateur à l'aide d'un faux SMS contenant un lien hypertexte ou un numéro à appeler où les informations confidentielles lui sont demandées. Dans la version vishing (contraction de voice et de phishing), c'est un utilisateur de Voice over IP qui est invité à appeler un serveur vocal qui va récupérer ses informations confidentielles.

Modes de traitement

Il est fondamental d'informer très rapidement et clairement les clients du risque encouru et de leur fournir tous les éléments leur permettant de déjouer l'arnaque. Cela peut être fait par tout moyen : courriel, courrier papier, éditorial en home page du site, article ou page de publicité dans la presse, etc.

Pour les entreprises fréquemment attaquées comme les banques, la communication doit être permanente et doit avoir une dimension pédagogique du client sur ce risque précis.

Les conseils de vigilance à rappeler :

- contrôler l'adresse du mail ou du site

- utiliser un firewall et un filtre anti-spam

- ne jamais donner d'information confidentielle en réponse à un mail

- ne pas cliquer sur un lien contenu dans un mail douteux, mais préférer se connecter directement à partir de son navigateur Web

- mettre à jour son système d'exploitation et son navigateur de manière régulière ; les versions les plus récentes incluent des outils anti-phishing.

L'affichage de la politique des e-mails sortants de l'entreprise est également recommandée. Elle doit bien sûr inclure le fait qu'aucune demande d'information sensible ou personnelle ne peut être initiée par mail. Elle peut aller jusqu'à la personnalisation des courriers permettant de réduire le risque en incluant des informations que les pirates ne peuvent pas avoir.

Les banques ont de leur côté développé des sites particulièrement sécurisés pour les virements en ligne.

Fiche de relevé d'incident

Phishing

Profil de l'organisation
Secteur : banque
Effectif : Plus de 1 000 salariés
Couverture géographique : Implantation physique internationale

Nature de l'incident/de la menace
Phishing
Année de l'incident : 2009

Exposé de l'incident
Détection le 27/08/2009, 12h30 par analyse des SpamTraps (e-mails créées spécifiquement pour recevoir les spams).
Le site de phishing impactant le groupe est identifié à une adresse .com.

Service interne ayant été mobilisé :
Unité spécialisée dans la sécurité Internet

Modes de traitement
Analyse de la criticité qui s'avère moyenne au vu du nombre de spams et de l'analyse des logs. La crise est donc gérée par l'unité spécialisée. En cas de criticité plus importante, une cellule de crise aurait été créée (selon les besoins : opérationnels, informaticiens, juristes, communicants).

Procédure :
Mise en œuvre de la procédure de fermeture du site de phishing.
Communication au réseau de correspondants de l'unité (communauté interne identifiée)
Préconisation de communication interne (ce cas ne nécessitait pas une communication externe spécifique).

Recours à des prestataires extérieurs privés :
Mandat donné à une société spécialisée pour la fermeture du site frauduleux

Résultats
Fermeture du site frauduleux obtenue en moins de 4h
Identification de l'origine : Maroc.
Mesures prises à l'issue de l'incident : analyse des logs pour détection clients piégés (<20) et contact de ces clients.

H. Usurpation / détournement de marques / contrefaçon

Fiche de relevé d'incident

Contrefaçon de marques / produits

Profil de l'organisation

Secteur : Site de vente aux enchères pour particuliers / Sociétés du secteur mode-luxe

Description de l'incident

De nombreux produits contrefaits (reproductions ou imitations) sont en vente sur Internet. Les marques ainsi spoliées contre-attaquent le plus souvent par des procédures juridiques. Au-delà de cet aspect, il est intéressant de regarder comment une partie mise en cause peut déplacer le débat sur le terrain de la communication et de la défense du consommateur.

Un site d'enchères en ligne bien connu mis en cause par des sociétés du secteur du luxe a connu dans ce type d'affaires, deux jugements en apparence contradictoires.

Dans une première affaire, une grande marque de cosmétiques avec un réseau de distribution non sélectif a ainsi été déboutée de son action, parce que le site incriminé avait mis en place des moyens de lutte contre la contrefaçon, faisant ainsi preuve de sa loyauté vis-à-vis des fabricants.

Dans un deuxième cas, le même site d'enchères (qui a fait appel) a été condamné successivement pour contrefaçon, utilisation abusive des noms de marques dans des mots-clés de recherche (constituant également une contrefaçon) et actes illicites portant atteinte au réseau de distribution sélective des sociétés demanderesses. En effet, il a été acté que le dit site ne possédait pas la seule qualité d'hébergeur et ne pouvait en conséquence bénéficier des dispositions de l'article 6.1.2 de la loi du 21 juin 2004 portant sur la confiance dans l'économie numérique.

Ces affaires présentent une double lecture : les fabricants estiment que le site de vente aux enchères nuit à leurs intérêts et à leur image de marque. D'un autre coté leurs attaques constituent une menace pour la réputation et le modèle économique du site visé.

Services internes mobilisés : service de communication, services juridiques.

Recours à des prestataires extérieurs privés : cabinet spécialisé en droit des marques, agences de relations publiques, solutions de veille économique, cabinet d'intelligence économique.

Modes de traitement

Pour le site d'enchères en ligne :

Il s'agit en premier lieu de se défendre en justice mais aussi d'apparaître comme le défenseur des droits fondamentaux des consommateurs, sans être considéré comme le complice d'agissements malhonnêtes. Parmi les actions lancées pour atteindre ces objectifs :

- communication autour des moyens de lutte contre la contrefaçon entrepris par le site de vente aux enchères avant les jugements.
- sortie d'un livre blanc sur les mesures de filtrages des contenus, publié les jours des plaidoiries.
- mise en avant du droit fondamental du citoyen à participer à la libre circulation des objets dans un monde commercial multipolaire.
- mobilisation du forum de discussion du site pour échanger avec les utilisateurs du service

- pétition envoyée par email à des millions d'utilisateurs demandant « la fin des pratiques commerciales déloyales » et proposant aux signataires de « *défendre leur droit à vendre leurs possessions et à accéder à des offres intéressantes parmi une sélection la plus large possible* » (signée par 750 000 personnes).
- lobbying auprès des instances européennes pour que les règlementations concernant la distribution sélective ne soient pas réformées dans un sens plus contraignant.

Pour les marques :
Les sociétés victimes de contrefaçon agissent en général avec des méthodes "traditionnelles" :
- action juridique
- campagne de communication en coordination avec les pouvoirs publics et les organisations professionnelles expliquant les risques de la contrefaçon pour les consommateurs (notamment la responsabilité pénale du vendeur et de l'acheteur), le défaut de qualité du produit vendu et les atteintes à la réputation de la marque.
- lobbying aux niveaux national et international.
En revanche, une participation plus active aux forums de discussions pour faire valoir le bien-fondé de leur position dans un échange direct avec les consommateurs pourrait probablement renforcer leur image de marque.

Résultats
Si la justice a donné gain de cause aux marques, qui ont obtenu, avant appel, des dommages et intérêts, le site de vente aux enchères a renforcé, par ses actions, son image de défenseur du petit consommateur face à des industriels insensibles, déniant le droit de chacun à disposer de ses biens comme bon lui semble.
Les principales décisions prises par les juges sont :
- dommages et intérêts évalués de façon forfaitaire et non pas selon le préjudice réel (ce mode d'évaluation est normalement réservé à des affaires de pure contrefaçon, ce qui n'était ici pas le cas)
- diffusion immédiate de l'arrêté du jugement dans trois publications nationales et internationales, ainsi que sur le site d'enchère source et national.
- règlement financier de tous les jugements rendu en dommages et intérêts avec l'obligation de régler les frais de procédures du plaignant.
- ordonnance d'injonction de cesser la mise en vente des produits sous peine d'une astreinte forfaitaire par jour de retard adjoint à une amende supplémentaire pour chaque infraction constatée.

I. Piratage de site

Description de l'incident

Dans la majorité des cas, les actes de piratage informatiques sont traités par les entreprises dans la plus grande discrétion. Il arrive cependant qu'ils aient un impact sur la réputation de l'entreprise, par exemple :

- Lorsqu'un hacker seul ou en groupe communique sur une opération d'intrusion ou de piratage réussie afin de valoriser ses exploits. Dans ce cas, l'image de l'entreprise est altérée par son incapacité de l'entreprise à protéger son système et ses données. Cette situation pourra être d'autant plus délicate si le piratage concerne des données financières comme ce fut le cas lors de vol de fichiers clients ou de numéros de carte de paiement.
- Lorsque des vulnérabilités du système d'information de l'entreprise sont présentées par un groupe de « gentils hackers » aux responsables de l'entreprise afin que celles-ci soient corrigées mais que rien n'est fait. Outre les risques d'intrusion et de vol de données ou de paralysie du système, les risques en termes d'image peuvent être importants du fait de l'audience des ces groupes sur les sites spécialisés.

Modes de traitement

Après la mise en œuvre des mesures adaptées en termes de sécurité informatique, il est important d'établir un plan de communication adaptée au contexte. Le service communication de l'entreprise sera donc placé en tête de pont, surtout si l'information relative à une intrusion ou un vol de données a été publiée.

Dans le cas de simple correction de vulnérabilité, un simple échange « amical » avec le groupe de hackers pourra être considéré comme une mesure suffisante.

Fiche de relevé d'incident

Piratage de site / Atteinte à l'image d'une entreprise

Profil de l'organisation
Secteur : Activités financières et d'assurance
Effectif : Plus de 1 000 salariés
Couverture géographique : Implantation physique et présence commerciale internationales.

Nature de l'incident/de la menace
Détection d'une faille de sécurité sur le site Internet
Année de l'incident : 2002

Exposé de l'incident
Le Webmaster et le responsable du site Internet de la société reçoivent un mail informant d'une faille de sécurité laissant l'accès aux données personnelles des internautes communiquant avec la société (candidats, prospects, etc.). Les auteurs sont des « gentils » hackers qui peuvent cependant mettre à mal l'image des entreprises par leur audience sur les forums et la reprise de leurs trouvailles dans la presse. Il y a également un risque juridique du fait des données en jeu.

Services internes ayant été mobilisés : Equipe responsable du site Internet, Direction Communication, Direction sécurité informatique, Direction informatique.

Modes de traitement : Technique, Communication
- Contact immédiat avec les auteurs du mail. Information faite sur les mesures prises.
- Parallèlement action rapide en interne avec mobilisation des compétences nécessaires (début août…)

Résultats
Délai entre le constat et la résolution : une semaine pour la résolution technique.
Le seul impact a été une mention sur le site des hackers dans une liste des entreprises qui « avaient des failles importantes, mais qui les ont corrigées ». Parallèlement, des entreprises ayant la même faille ont été stigmatisées (copie d'écrans, articles assassins repris dans de multiples sites et forums) pour la non réaction à cette intrusion.

Identification de l'origine
Mail envoyé par le hacker au Webmaster et au responsable du site signalant les failles

Mesures prises à l'issue de cet incident
1 mois après avec plan d'action allant bien au-delà du problème original :
- révision des normes de développement ;
- recherche de vulnérabilités obligatoires sur environnement de qualification ;
- politique de tests d'intrusion (confiés à une société externe) sur tous les sites extranet et Internet ;
- mise en place d'une réunion bimensuelle sur les impacts des failles publiées.

J. Flogs

Description de l'incident

Les Flogs ou Fake Blogs ou Flack Blogs sont des blogs qui se disent impartiaux, indépendants, autonomes et qui en fait sous couvert de cette impartialité apparente cherchent à promouvoir de façon déguisée une société, une marque, des produits ou services commerciaux ou bien encore une idéologie. Les Flogs ne représentent pas en eux-mêmes un incident d'e-réputation, mais en revanche, la découverte de la supercherie que représente un Flog peut constituer un incident majeur pour la société qui l'a initié.

De grandes marques y ont été confrontées, essayant de développer une stratégie de communication en ligne sur les médias de type Web 2.0.

L'utilisation de Fake Blogs est considérée comme une manœuvre malhonnête visant à abuser les internautes et les blogueurs afin de profiter de l'essence même des médias participatifs et du Web 2.0. Lorsque ce type de manipulation est découvert, un buzz négatif visant à exposer la tentative et à faire paraître l'entreprise sous un mauvais jour est souvent mis en place par les personnes ayant été abusées.

Un des premiers Flogs est « Walmarting Across America », un blog lancé en 2006 par Edelman, une société spécialisée dans les relations publiques, prestataire de Walmart et qui essayait de faire croire que ce blog avait été lancé et animé par deux fans de Walmart.

Service interne à mobiliser
Service Communication : souvent à l'origine de la décision de lancer un Flog, c'est ce dernier qui est le plus à même de réorienter la communication

Modes de traitement

C'est par la communication que les suites néfastes du lancement d'un Flog peuvent être traitées.

Il est bon de savoir que l'association WOMMA (Word of Mouth Marketing Association) et l'association Public Relations Society of America, dans leur code d'éthique, stipulent que l'authenticité et la transparence sont des éléments fondamentaux qui caractérisent la communication sur les réseaux sociaux et les blogs.

En tout état de cause, une fois qu'un Flog est découvert, la communication se devra d'être claire et honnête.

Fiche de relevé d'incident

Détection par le grand public de l'utilisation de Flogs à des fins de communication

Profil de l'organisation
Secteur : Restauration
Effectif : Plus de 1000 salariés
Couverture géographique : Implantation physique internationale, Présence commerciale internationale

Nature de l'incident/de la menace
Détection de l'utilisation de faux blogs à des fins de communication
Année de l'incident : 2006

Description de l'incident
Une grande chaîne de restauration rapide organisait un concours visant à collecter des vignettes afin de gagner des produits de la chaîne, ainsi que de nombreux lots. Deux blogs dits « indépendants » apparurent : l'un narrait l'obsession d'un participant et son envie de gagner, l'autre vantait le côté original et amusant du jeu, ainsi que les produits de la chaîne (variété des menus, gain de temps, *etc.*).
L'incident résulte dans le fait que ces blogs n'étaient pas indépendants, et qu'ils ont été identifiés comme tels.

Service interne à mobiliser : le service Communication

Modes de traitement
- Communication : Admettre l'origine des blogs, honnêteté de rigueur ; éventuellement, mettre en avant que l'intention n'est pas de tromper le consommateur, mais plutôt de communiquer de façon originale, en étant présent sur tous types de supports (proximité avec les consommateurs jeunes (cœur de cible), utilisant massivement Internet.)

Résultat
Suppression des blogs par la société.

K. Splogs

Description de l'incident

Les Splogs ou Spam Blogs sont des blogs souvent générés de façon automatisée et qui visent à générer du trafic. Ils affichent des bannières publicitaires ou des redirections vers des sites payants ou des sites de vente en ligne.

Les Splogs sont souvent utilisés pour rediriger vers des sites payants pour adultes, vers des boutiques de vente de contrefaçon. Il est à noter que le site marchand n'est pas forcément le responsable de la mise en place de ces Splogs. Ces mêmes sites reversent souvent des commissions à la vente ou au trafic, aux personnes disposant d'un compte « revendeur » ou « partenaire » : la manœuvre peut donc être réalisée par un ou plusieurs partenaires.

Ces Splogs utilisent souvent le nom de grandes marques, sources de trafic. Ainsi le préjudice fait à la marque est indirect : son nom est associé à du spam et à des produits pornographiques ou illégaux. Ces Splogs ont une durée de vie très courte allant de quelques heures à quelques jours.

Services internes à mobiliser

Service veille / Service Communication : mise en place systématique de détection de ces Splogs et action de premier niveau en signalant ces blogs comme illicites.

Modes de traitement

Ces Splogs sont souvent totalement illicites. Ils sont générés à partir de plateformes gratuites de conception de blogs en ligne et vont à l'encontre des Conditions Générales d'Utilisation, il suffit souvent de simplement les signaler à l'administrateur de la plateforme de blogs pour qu'ils soient supprimés.

Une action juridique pour utilisation illicite de la marque est possible mais peut s'avérer difficile à mener, ces systèmes reposant souvent sur des écrans successifs visant à masquer l'identité du spammeur, les zones géographiques des parties prenantes (entreprise / spammeur / hébergeur) étant souvent différentes.

Fiche de relevé d'incident

Détection par le grand public de l'utilisation d'un Splog à des fins de communication

Profil de l'organisation
Secteur : Agro-alimentaire
Effectif : Plus de 1 000 salariés
Couverture géographique : Implantation physique internationale, Présence commerciale internationale

Nature de l'incident/de la menace
Détection de l'utilisation de Splogs contenant des liens vers les sites marchands de la marque dans le but de promouvoir ces produits.
Année de l'incident : 2009
De nombreux liens pointaient vers les sites « commerciaux de la marque » en remettant ainsi en cause l'éthique de la société.

Service interne à mobiliser : le service Communication

Modes de traitement
Dans la plupart des cas, la marque n'est pas à l'origine de ces splogs, il s'agit d'intermédiaires qui touchent des commissions ; dans ce cas, il est essentiel de communiquer sur ce point, et demander de fermer ces blogs (souvent simple, en collaboration avec l'hébergeur des blogs incriminés).

Résultat
Disparition des blogs supprimés par l'hébergeur.

L. Cybergriping

Description de l'incident

La protection des noms de domaine directement affiliés à une entreprise, à ses enseignes ou ses marques est liée au contrôle de son identité numérique. Le cybergriping se définit comme l'action d'enregistrer un nom de domaine en reprenant le nom d'une marque ou d'une personne célèbre et en l'associant avec des termes péjoratifs pour nuire à la réputation de la marque ou de la personnalité visée (par exemple « XXXsucks.com » pour les sites anglosaxons ou « jedetesteXXX.com » pour des sites francophones).

Il est important pour l'entreprise de détecter ces actes de cybergriping de façon à intervenir en amont le plus rapidement possible et ainsi minimiser les conséquences de l'action néfaste (usurpation de marques en noms de domaine, contrefaçon…). Des solutions de veille automatique ou des prestations spécialisées permettent d'accompagner les entreprises dans cette démarche.

Acteurs de cybergriping

Dans la sphère de l'entreprise, les principaux acteurs propices aux actions de cybergriping peuvent être des clients mécontents, des salariés en conflit avec leur entreprise, ou encore des concurrents agressifs qui visent la déstabilisation de l'entreprise ciblée.

Instances de régulation et de médiation

L'Organisation Mondiale de la Propriété Intellectuelle arbitre les litiges relatifs aux actes de cybergriping et cherche les solutions permettant de protéger efficacement les préjudices et les actes de malveillance en ligne qui se multiplient avec Internet et l'évolution des technologies de l'information. Lorsque le nom de domaine litigieux est confondu avec la marque et lui porte atteinte, l'OMPI peut ordonner par son centre d'arbitrage et de médiation le transfert du nom de domaine vers la société incriminée.

Principales entreprises cibles victimes de cybergriping

- Les grandes marques ou les grandes entreprises qui génèrent des buzz et contre-buzz sur Internet à partir d'opérations de communication et de promotion de masse ;
- Les sociétés innovantes (« nouveaux entrants », start-up…) qui se positionnent sur des marchés émergents impliquant une captation de clientèle rapide et massive à partir d'actions de communication et de promotion innovantes sur Internet.

Modes de traitement

- Actions de prévention pouvant être mises en œuvre :
    - Déposer les noms de domaine courants (.com, .fr, .net, .eu, .info, .pro….) et ceux où l'entreprise est positionnée à l'international (.de, .es, .cn….) : ceux liés au nom de l'entreprise, à ses enseignes et à ses marques, à ses slogans ou encore aux termes clés qui sont associés à son « périmètre Image » ;

- Mettre sous alerte ses noms de marques sur les dernières publications Web pour être averti quasiment en temps réel des publications de sites pouvant incriminer ses marques (outils adaptés à la veille de marque sur Internet…). Ces actions peuvent être plus complexes si la marque a une forte notoriété, si elle est peu distinctive car liée à une multitude de mots génériques, ou s'il faut surveiller une majorité de sites à l'international ;
- Surveiller le dépôt de noms de domaine avec une orthographe approchante ou avec l'ajout de suffixes, de préfixes, d'expressions ou de slogans liés à l'entreprise ou à ses marques (surveiller également le changement de contenu car les noms de domaines ne mènent pas toujours à un site) ;
- Utiliser les flux RSS permettant la reproduction automatique du contenu de certains sites (identifier également les acteurs de la chaîne de responsabilité de manière à agir sur les points sensibles en intimidation ou en action juridique).

- Traitement et actions curatives possibles :
  - Créer son propre site de retours de clients afin de gérer et maîtriser les messages négatifs ;
  - Diminuer la visibilité des sites : des sociétés spécialisées en e-réputation interviennent pour la création de sites et de contenus pouvant positionner une entreprise en première place dans les pages résultats des moteurs de recherche, saturer des réseaux sociaux, ou encore publier des contenus positifs dans des sites référents qui concernent l'entreprise ;
  - Dialoguer avec les responsables éditoriaux et les propriétaires du site Internet en question.

Fiche de relevé d'incident

Acte de cybergriping

Description de l'incident

Création d'un site de dénigrement d'une marque avec un nom de domaine utilisant le nom de la marque et un terme péjoratif (XXXsucks.com)

Services internes à mobiliser : la Direction juridique, le Service de Veille, le Service Communication, le Service Relation Consommateur, et la Direction de la stratégie.
Services externes à mobiliser : un cabinet spécialisé dans la propriété industrielle et la protection des noms de domaine Internet.

Modes de traitement

- Juridique : déposer une plainte auprès du Centre d'arbitrage et de médiation de l'OMPI par courrier électronique et par support papier. Demander la vérification d'enregistrement et l'infraction au droit des marques
- Technique : assurer une veille sur les dépôts de noms de domaine proches du nom de l'entreprise et de ses marques, et des changements de contenu pour intervenir si nécessaire. Limiter le ranking du site incriminant en achetant des mots-clés ou des noms de domaine proches du vocabulaire usité par l'attaquant.
- Relation Client : préparer un argumentaire pour contrer le site de cybergriping incriminant, mettre en cause l'aspect subjectif et subversif du site.
- Stratégique : racheter le nom de domaine auprès du particulier ou de l'entreprise qui a lancé l'acte de cybergriping si le dépôt de plainte ne peut pas conduire au retrait du site incriminant (accord à l'amiable…).

Fiche de relevé d'incident

Référencement malveillant sur un site pornographique

Description de l'incident

Référencement malveillant sur un site pornographique
Le Webmestre a détecté cet incident lors des actions de référencement classique du site Internet de l'organisme. Ce référencement est malveillant car il nécessite une action manuelle d'inscription sur le site en cause.

Modes de traitement

Aucun traitement, le site de l'organisme est toujours référencé par un site pornographique.
La gestion de cet incident n'est pas la priorité. Les préoccupations des publics visés des 2 sites étant sans rapport, il a été jugé que la réputation scientifique de l'organisme n'était pas gravement altérée.

M.Cybersquatting

Description de l'incident

Le Cybersquatting est une démarche visant à faire l'acquisition de noms de domaine reprenant explicitement le nom d'une marque ou d'un produit sur une ou plusieurs extensions avant que l'entreprise n'en fasse elle-même l'acquisition.

Le Cybersquatting peut alors être utilisé de deux façons :

- Il est utilisé afin de vendre des produits ou générer des revenus tirés de programmes de publicité en ligne.
- Il est « parké », c'est-à-dire confié à un gestionnaire de « Domain Parking » et proposé à la revente.

Selon les produits vendus sur le nom de domaine cybersquatté ou les publicités diffusées, cela peut avoir un impact négatif sur l'image de marque de la société.

Un exemple de cas célèbre est le nom de domaine www.france2.com qui est encore aujourd'hui un nom de domaine cybersquatté en Domain Parking.

Services internes à mobiliser

Service juridique

Modes de traitement

Le traitement lié au cybersquatting est complexe. La jurisprudence est encore aujourd'hui évolutive et fait par ailleurs référence à plusieurs notions :

- L'antériorité de la marque par rapport au nom de domaine
- La confusion possible entre les activités de la société « légitime » et du cybersquatteur

Par ailleurs, un accord à l'amiable peut s'avérer plus rentable que le lancement d'une action en justice dont l'issue pourra s'avérer incertaine.

Recours à une administration ou autorité publique

L'ICANN, autorité de régulation des noms de domaine, s'engage à arbitrer en ligne un litige lié aux noms de domaine sous 60 jours. Elle s'appuie pour cela sur différents organismes qui sont en charge de la gestion des dossiers de conflits. Le WIPO est un de ces organismes.

III. Maîtriser et protéger l'identité numérique de son organisation

A. Mesures préventives

1. Règles déontologiques internes

Le développement de l'Internet a généré de nouveaux modes de consommation de l'information. Du stade de consommateurs, les individus deviennent producteurs d'information. L'Internet participatif a engagé l'internaute dans un processus de co-production (les User Generated Content) et de rétroaction avec son environnement par les commentaires et les interventions sur les forums notamment. Il est à noter que cette tendance qui se dessine sur les usages numériques part de la sphère privée et vient impacter les usages dans la sphère professionnelle. On assiste à un effacement des 2 sphères pour ne constituer au final qu'un environnement global dans lequel les individus prennent la parole.

L'une des représentations les plus manifestes de cette prise de parole réside dans le fait communautaire ou l'appartenance des individus à un ou des réseaux sociaux. Ainsi, selon une étude réalisée par Novametrie[8], 92 % des salariés en France sont présents sur les réseaux sociaux numériques.

De ce point de vue, les pratiques individuelles sont en avance sur celles des entreprises. La prise de parole n'est pas "bridée" : elle dénote une spontanéité assumée dans les classes d'âges les plus jeunes. La lecture du message final peut prêter à interprétation. L'avis subjectif peut se confondre avec une analyse objective des faits.

On l'aura vite compris, les entreprises portent un intérêt croissant au développement des réseaux sociaux numériques à des fins de surveillance de leur environnement, mais aussi d'un point de vue de la sécurité pour ne pas être prises à défaut en matière de confidentialité lorsque des collaborateurs interviennent sur ces réseaux.

Suivant le principe que mieux vaut prévenir que guérir, les entreprises sont engagées dans un processus de balisage des usages numériques de leurs salariés. Il s'agit en l'occurrence de proposer aux salariés une charte d'utilisation de ces réseaux. La graduation des engagements sollicités peut aller d'un simple renforcement de la clause de confidentialité dans les contrats de travail à une interdiction d'accès à ces réseaux.

Les entreprises vont-elles pour autant vers la mise en place de codes déontologiques quant à l'usage des réseaux sociaux numériques ou de charte d'utilisation de ces réseaux ? L'observation des tendances récentes montre une volonté des entreprises de maîtriser davantage la communication des salariés. Des politiques RH sont désormais envisagées pour intégrer cette nouvelle donne. Cependant, on constate de fortes spécificités, en fonction du secteur, du point de vue de la taille de l'entreprise, de la pression concurrentielle, des relations qu'elle entretient avec son environnement et bien sûr de la nature des relations sociales qui y prévalent.

[8] 1er baromètre des Stratégies Rh et des réseaux sociaux – Novamétrie – Digital Jobs – septembre 2009

A minima, il semble qu'un consensus se dégage auprès des Directions des Ressources Humaines pour y inclure les items suivants[9] :

- le "dégagement de responsabilité" (*Disclaimer*) soit la référence au fait que le salarié intervient à titre personnel et n'engage pas la responsabilité de son entreprise
- l'engagement de ne pas révéler d'informations sensibles
- le respect des droits de propriété intellectuelle qui consiste à toujours citer les sources
- le fait de ne pas dénigrer les personnes comme les organisations
- le fait de porter des jugements "mesurés" qui ne risquent pas de porter préjudice à l'entreprise.

Il convient de suivre avec attention la mise en place de ces politiques RH qui, on peut le penser, impacteront la nature des contrats de travail.

2. Surveillance de l'environnement

La surveillance de l'environnement est un élément clé dans un processus de gestion de l'identité numérique de son entreprise. L'objectif d'une telle démarche est de pouvoir capter et analyser toutes les informations susceptibles de pouvoir entacher à un moment ou à un autre l'image de l'entreprise. Dès lors, chaque signal doit être traité, analysé afin d'appliquer les actions adéquates et ainsi anticiper l'apparition d'une future crise.

Dans un premier temps, il est impératif de pouvoir établir un spectre de surveillance aussi large que possible. Se pose alors la question du « sourcing », c'est-à-dire des sources à surveiller. Les principales sources à surveiller sont la presse générale et spécialisée, les sites métiers, les blogs, les forums de discussions ainsi que les réseaux sociaux. De nouvelles sources d'information telles que le site Twitter sont également à suivre avec attention car elles permettent la diffusion d'une information, qu'elle soit avérée ou non, à une vitesse vertigineuse. De multiples solutions logicielles présentées au §4 existent afin de répondre à ce besoin.

Ensuite, il convient de traiter et d'analyser les informations qui auront été préalablement collectées sur les sources ciblées. L'objectif est alors d'identifier des signaux faibles, c'est-à-dire des informations noyées dans la masse d'information accessible mais qui, si rien n'est fait, peuvent nuire à l'entreprise.

Enfin, il est impératif d'étudier avec les services compétents (Direction générale, Communication, Service juridique, stratégie, etc.) les mesures à mettre en œuvre.

En conclusion, la mise en place d'une démarche suivie de veille pilotée par des experts du sujet doit permettre d'éviter l'apparition de crise majeure par la mise en place en amont d'actions de contre-mesure adaptées au fil de l'eau.

[9] Voir à ce sujet une base de données en ligne qui recense auprès d'une centaine d'entreprises et d'institutions US les chartes d'utilisation des réseaux sociaux et autres espaces numériques susceptibles d'être utilisés par les salariés : Social Media Governance (http://socialmediagovernance.com/policies.php)

3. Utilisation des réseaux (réseaux numériques ou humains)

Quelles que soient les mesures préventives mises en œuvre, il est impératif de s'appuyer tant sur les réseaux numériques qu'humains.

En matière de surveillance, et comme il l'a été indiqué dans le paragraphe précédent, le suivi des réseaux numériques est aujourd'hui une étape fondamentale. Les sources dites « Web 2.0 », en l'espèce les blogs, forums et réseaux sociaux, véhiculent une multitude d'informations tant sur la société, ses produits, ses collaborateurs et qui peuvent nuire à l'entreprise.

Le suivi des réseaux humains n'est toutefois pas à négliger. Il est de ce fait très important de suivre la perception que l'on peut avoir de l'entreprise à l'extérieur en participant à des associations professionnelles, des salons, ou pour savoir ce que l'on pense des produits en allant sur le terrain interroger clients ou fournisseurs. En interne, pour connaître l'état d'esprit des collaborateurs de l'entreprise, il est utile de maintenir des contacts privilégiés avec les représentants du personnel et les délégués syndicaux.

En matière d'actions de contre-mesure suite à l'identification d'un signal faible, il est très utile d'utiliser ces deux types de réseaux. Pour les réseaux numériques, de multiples actions peuvent être mises en œuvre telles que la création de blogs pour passer un message défensif ou offensif, la publication de messages ciblés sur des blogs ou des forums référents, la diffusion de communiqués de presse. Les réseaux humains peuvent également être des relais très efficaces pour la mise en place des telles actions. On pourra ainsi passer des messages officieux ou diffuser des dossiers « confidentiels » à des délégués syndicaux ou des représentants du personnel, ou à l'extérieur à des élus ou des journalistes. Notons que les liens entre ces deux types de réseaux sont souvent étroits et que les interconnexions sont souvent nombreuses.

B. Mesures curatives

Une fois l'atteinte à la réputation d'une entreprise constatée, il convient dans un premier temps d'en définir le type, puis d'étudier son évolution pour tenter d'en identifier la source afin de mettre en œuvre les recours adaptés.

1. Identifier une rumeur ou une action de désinformation

Comme vu précédemment, dans un contexte de guerre de l'information, les entreprises et organisations se doivent de définir la nature des réponses à apporter pour protéger leur identité numérique. Une analyse de la typologie des risques informationnels a permis d'identifier les facteurs qui favorisent les attaques sur la notoriété de l'organisation : l'accélération du cycle de l'information, la numérisation croissante des contenus, le développement des données produites par les individus.

Le traitement peut être de nature juridique. Cependant l'échelle temps n'est pas la même entre la propagation de l'attaque et la mise en branle de l'arsenal judiciaire. Qui plus est la réponse peut engendrer une série d'effets pervers par rapport à l'événement constaté et mener à une surenchère dans le processus de désinformation. Il peut être technique et viser à neutraliser les ressources de « l'attaquant ». Il peut être organisationnel avec la mise en place d'une "war room"

qui agrège l'ensemble des ressources présentes dans l'organisation susceptibles de traiter l'attaque.

Cependant, le traitement – aussi impératif soit-il – ne peut occulter la nécessaire réflexion sur l'anticipation de la crise. Les organisations qui maîtrisent leur identité numérique sont celles qui ont adopté une démarche structurée : il s'agit de cartographier les risques potentiels, de définir les règles déontologiques internes via la mise en place de chartes d'utilisation pour les collaborateurs quant à l'usage des réseaux ouverts, de repérer les relais d'information nécessaires à toute procédure de prévention des risques informationnels, d'optimiser la communication avec son premier cercle de sous-traitants, fournisseurs et principaux clients et au final de mettre en place un système de capteurs pour la détection des signaux.

Malgré toutes les précautions prises par l'organisation, le risque demeure. Lorsque l'action de désinformation est engagée, il s'agit pour l'organisation d'être réactive dans les plus brefs délais. L'espace temps du numérique se confond avec le temps réel (hot news). Une fausse information, une rumeur ou encore une opinion négative sitôt produite peut être immédiatement relayée et propagée sur le net. De ce point de vue, le média Internet fonctionne comme une caisse de résonnance qui dans un système de gestion des flux tend à favoriser la reproduction et la duplication des messages pour une rediffusion massive par l'intermédiaire des liens de quelque nature qu'ils soient (liens hypertexte, rétroliens, flux RSS, Retweet, *etc.*) C'est ce qu'il est commun d'appeler l'effet "buzz". Cette amplification peut éventuellement être accentuée lorsque les médias traditionnels tels la presse, la télévision ou la radio reprennent ces informations.

Détecter les prémices de la rumeur est devenu un impératif pour les entreprises et les organisations, voire les individus les plus exposés médiatiquement. Evaluer les réactions possibles et identifier les critiques potentielles, c'est être plus efficace dans la capacité d'une entreprise à les marginaliser. Pour ce faire, chacun peut disposer d'un arsenal d'outils qui permettent de détecter en quasi temps réel les attaques portées à sa réputation. Il s'agit dès lors – dans le meilleur des cas - d'extraire de la masse informationnelle les signaux faibles qui préfigurent l'attaque. Soit, mener une action de surveillance systématique (en ligne) sur le média Internet et suivre tous les signes susceptibles d'annoncer une réaction amplifiée sur le net.

L'organisation de la surveillance devient un enjeu majeur pour les acteurs potentiellement soumis au risque de déstabilisation et d'atteinte à son intégrité, donc son image. Ceci est d'autant plus manifeste, que notre société est entrée dans un contexte de valorisation des actions et des projets par des techniques de communication de plus en plus sophistiquées. Il devient ainsi commun de voir des groupes du CAC 40 organiser leur communication institutionnelle (corporate) autour de techniques narratives qui organisent leur univers de représentation dans un récit, une histoire qui se raconte.

Cependant, organiser sa surveillance de manière efficace demande de la méthode et du bon sens ; on ne négligera pas cependant, la part d'imprévu qui ouvre le champ des possibles en étendant l'investigation dans les points aveugles de nos représentations habituelles. Mais pour revenir à la détection du prévisible, on retiendra les étapes suivantes comme étant nécessaires au formatage du processus de surveillance :

- la cartographie des espaces les plus sensibles sur le net susceptibles de diffuser une rumeur pour mettre à mal la réputation de l'entreprise ;
- la nécessité de « sourcer » les sites à risques ;
- la définition précise et rigoureuse des axes de surveillance à suivre. Il s'agira de retenir les mots-clés et thèmes qui feront l'objet d'un suivi ;
- le paramétrage des alertes automatisées ;
- l'analyse de la tonalité sur des thèmes de recherche ;
- l'analyse de la popularité sur certaines requêtes ;
- le suivi des leaders d'opinion (blogs influents, leaders de communautés …) ;
- le suivi des forums.

Qu'il s'agisse d'effectuer une surveillance d'opinion, de sa réputation, ou encore de son identité numérique, la réalisation de ces tâches peut être traitée en interne dans le cadre d'une direction ou d'un service intelligence économique qui intègre une cellule de gestion de crise. Historiquement, certains groupes localisent cette cellule au niveau d'une Direction de la communication qui pilote la communication corporate et l'identité de l'entreprise. D'autres organisations privilégieront la sous-traitance de la surveillance à une société spécialisée ou encore à une agence de communication qui dispose d'un service dédié à ce type d'activité.

L'accélération des flux informationnels conjuguée à une excroissance significative du volume de données à traiter (notamment de données non structurées) nécessite le recours à des outils et logiciels qui vont automatiser ces tâches, permettre l'extraction dans des contenus hétérogènes et favoriser l'analyse des signaux récupérés par des techniques de catégorisation et ou de visualisation. Des logiciels qui vont aussi assurer :

- la traduction des contenus ;
- le croisement de divers univers sémantiques pour donner sens à des données a priori non corrélées ;
- la contextualisation des données pour une mise en perspective.

En tout état de cause, une surveillance efficace est une question de méthode et d'outils, en définissant lors d'une analyse préalable, les thèmes et sources à surveiller.

2. Quels recours pour quelles actions

Les recours juridiques sont précisés dans le chapitre suivant.

IV. La réputation à l'épreuve de la diffamation, de l'injure et du dénigrement[10]

Il est plus facile de garder intacte sa réputation que de la blanchir quand elle est ternie.
Thomas Paine,
Il est presque toujours en notre pouvoir de rétablir notre réputation.
François de La Rochefoucauld
Pour un mot, un homme est réputé sage ; pour un mot, un homme est jugé sot.
Confucius

Certes, la réputation relève de l'opinion émise par une personne vis-à-vis d'une autre. Celle-ci peut être positive ou négative. Rarement on cherchera à neutraliser ou éradiquer les effets d'une critique positive. En revanche, lorsqu'elle est négative, il faut des outils qui permettent de collecter ou recueillir les traces des atteintes car en la matière si l'on doit aller sur le terrain judiciaire il faut avoir la preuve de ses allégations. Le droit ne supporte ni les approximations ni les affirmations.

Ainsi, les mesures juridiques sont aussi la voie de recours pour supprimer les atteintes à la réputation. Leur efficacité est certaine lorsqu'elles ne sont pas prescrites. Ces mesures doivent être employées soit pour obtenir la suppression des propos mettant en cause directement l'entreprise ou ses produits et services, soit dans une perspective punitive et réparatrice.

Concrètement, il faut rechercher si la contenance des propos est susceptible de porter atteinte à la réputation d'une entreprise ou d'une personne et d'écarter les cas où elle n'est que la juste émanation d'une liberté d'expression et de critique offerte à tous, principe maintes fois évoqué. Si ce n'est pas le cas, il doit d'abord être procédé au constat des faits (A), puis à l'identification de l'auteur des messages litigieux (B), puis qualifier leur nature juridique (C) et enfin, envisager la responsabilité de l'auteur et du directeur de publication (D).

A. Conserver les traces de l'atteinte à la réputation

Avant toute chose, lorsqu'une personne découvre que l'on porte atteinte à sa réputation, elle doit en conserver la preuve, base essentielle de toute action judiciaire future. En effet, cette mesure est nécessaire car elle permet à la fois d'obtenir une date certaine de publication, essentielle dans les cas de diffamation, et d'assurer la matérialité de faits en raison de la volatilité du Web.

[10] Ce chapitre a été rédigé par Maître Gérard HAAS, Docteur en droit, Avocat à la Cour d'appel de Paris, Spécialiste en propriété intellectuelle

La date de publication des propos sur le site Internet est fondamentale puisqu'il faut rappeler que dans le cadre d'une diffamation et en application de l'article 65 de la loi de 1881, le délai de prescription de trois mois court à compter de la première publication.

Ce délai fort bref oblige toutes les personnes exposées à surveiller la Toile, pour ne pas découvrir trop tard une atteinte à leur réputation qui ne pourra plus être délogée parce que prescrite.

Pour pouvoir se défendre, la victime doit avoir une réaction active et faire constater la diffusion des propos litigieux par exemple par l'Agence pour la protection des programmes (APP) ou encore par tout huissier compétent. Pour qu'il soit efficace, ce constat devra décrire étape par étape l'acheminement suivi de la page d'accueil du site à la page où les propos litigieux figurent.

A ce stade, il est primordial de rechercher la personne responsable de la publication ou à tout le moins son pseudonyme. Certes, c'est d'abord l'auteur de l'écrit litigieux qui est responsable, mais l'opacité de la Toile peut rendre cette identification particulièrement complexe. Aussi, on veillera à ce qu'il soit procédé au constat des mentions légales afin de déterminer qui est le directeur de publication et l'hébergeur du site où lesdits propos se sont tenus.

Le constat, une fois établi, assure à la victime la preuve de la date de publication des propos litigieux. Il convient maintenant d'identifier l'auteur des propos.

B. Identifier l'auteur des propos litigieux

Le parcours d'un internaute laisse des « traces » numériques susceptibles de l'identifier. Cette identification s'avère possible si les données de communication électronique sont conservées.

Or, le décret du 24 mars 2006 relatif à la conservation des données de communications électroniques issue de la loi n°2004-575 pour la confiance dans l'économie numérique (LCEN) fixe la durée de conservation des données par les fournisseurs d'accès à Internet et d'hébergement à un an.

Cette obligation de conservation recouvre la moindre modification d'un quelconque contenu hébergé, y compris les informations permettant d'identifier quiconque a contribué à la création du contenu ou de l'un des contenus des services dont les fournisseurs d'accès à Internet et les hébergeurs sont prestataires en vertu de l'article 6-II de la loi LCEN.

Cette obligation est sanctionnée pénalement par un an d'emprisonnement et 75 000 euros et le quintuple de l'amende pour une personne morale (article 6-VI de la loi LCEN). Son non-respect peut aussi constituer une faute civile sur la base des articles 1382 et 1383 du Code civil.

Ainsi, une victime peut saisir le président du tribunal compétent par une requête ou un référé sur le fondement de l'article 145 du Code de procédure civile afin de faire ordonner la communication des données d'identification de l'auteur desdits propos. Il pourra même être demandé à l'autorité judiciaire d'ordonner à l'hébergeur ou à défaut aux fournisseurs d'accès Internet de supprimer les propos tenus en application de l'article 6-I.8 de la loi LCEN.

Chacune de ces procédures se heurte à des inconvénients et avantages à prendre en considération :

- La requête a l'avantage d'être une procédure rapide revêtant un caractère non contradictoire en vertu de l'article 493 du Code de procédure civile. Toutefois, celle-ci doit être motivée, notamment en ce qui concerne son caractère non contradictoire sous peine de ne pas aboutir. Elle peut être directement envoyée aux personnes concernées puisqu'elle est exécutoire au vu de la seule minute, il n'est donc pas nécessaire alors de passer par la voie d'un huissier.

- Le référé est également une procédure rapide. Mais elle est contradictoire, ce qui signifie qu'elle peut se heurter aux contestations de l'adversaire.

L'identification de l'auteur pose un problème dans la mesure où un hébergeur n'est pas tenu de fournir les noms et adresses de l'éditeur d'un contenu en ligne. Or, sans cette information une action judiciaire est difficilement envisageable.

Lorsque l'on a la preuve de l'atteinte à la réputation, et l'identification d'une personne susceptible d'engager sa responsabilité, de ce fait il convient de qualifier exactement la nature des propos tenus.

C. Qualifier la nature juridique de l'atteinte à la réputation

L'atteinte à la réputation peut revêtir diverses formes :

- Diffamation
- Injure
- Dénigrement

L'article 29 de la loi du 29 juillet 1881 relative à la liberté de la presse définit **la diffamation** comme « *toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération d'une personne* », le fait imputé étant entendu comme devant être suffisamment précis, détachable du débat d'option et distinct du jugement de valeur pour pouvoir le cas échant faire l'objet d'une preuve et d'un débat contradictoire.

Ce délit qui est caractérisé même si l'imputation est formulée sous forme déguisée ou dubitative ou encore par voie d'insinuations se distingue ainsi de **l'injure**, définie par le même texte comme « *toute expression outrageante, termes de mépris ou invectives qui ne renferment l'imputation d'aucun fait* », comme de l'expression subjective d'une opinion, dont la pertinence peut être librement discutée dans le cadre d'un débat d'idées mais dont la vérité ne saurait être prouvée.

Concrètement, les éléments de l'infraction sont constitués lorsque :

- L'existence d'un reproche portant sur des faits précis et déterminés porte atteinte à l'honneur ou à la considération d'une personne ;
- Une intention de nuire qui se présume des faits eux-mêmes.

Néanmoins, soulignons que la personne accusée peut toujours prouver sa bonne foi afin d'éviter une condamnation. Cela suppose qu'elle puisse justifier la réunion des quatre conditions cumulatives suivantes:

- la légitimité du but poursuivi,
- l'absence d'intention de nuire,

- la prudence et la mesure dans l'expression,
- et enfin la vérification de ses sources.

Ainsi, la bonne foi pourra résulter de la preuve d'une intention de satisfaire le « droit de savoir » reconnu à autrui sous condition que les propos tenus soient exempts de toute animosité personnelle, préjudiciable à la personne visée.

Par ailleurs, rappelons que les imputations diffamatoires sont de droit, réputées faites avec intention de nuire, mais elles peuvent être justifiées lorsque leur auteur établit sa bonne foi, en prouvant qu'il a poursuivi un but légitime étranger à toute animosité personnelle, et qu'il s'est conformé à un certain nombre d'exigences, en particulier de sérieux de l'enquête ainsi que de prudence dans l'expression.

Le **dénigrement**, quant à lui, consiste à jeter publiquement le discrédit sur un concurrent en critiquant ses produits ou sa personnalité, afin de détourner sa clientèle ou d'en tirer un quelconque profit. Il constitue un acte de concurrence déloyale fondé sur l'article 1382 du Code civil dès lors que la critique émise est malveillante, démesurée et/ou systématique, et qu'elle ternit la réputation, l'image de la société visée.

Ainsi, il a été jugé que ne constitue pas du dénigrement :

- des appréciations même sévères, portées par un chercheur lors d'une interview dès lors qu'elles se cantonnent aux domaines scientifique et professionnel (CA PARIS, 1ere civ sect A, 26 mars 1990) ;
- le fait qu'un concessionnaire fasse connaître au client démarché la date d'expiration de l'ancienne concession dès lors que cette allégation est exacte (Cass com, 2 mars 1999) ;
- les critiques exemptes de mauvaise foi d'un rédacteur d'articles gastronomiques (CA DIJON, 7 janvier 2004) ;
- le fait d'inviter le public à renoncer au port de la fourrure et à privilégier le synthétique lorsque la cruauté des images et les termes employés n'excèdent pas les moyens employés dans ce type de publicité (CA PARIS, 1ch section B 18 avril 1992).

En clair, il n'y a pas de dénigrement lorsque les propos sont objectifs et modérés et s'inscrivent ainsi dans le cadre d'une libre critique. En revanche, lorsque la critique est excessive ou encore subjective, il y a dénigrement. Il en est ainsi pour les cas suivants :

- de vives critiques contenues dans une bibliographie en dépit de la mise en garde des auteurs dès lorsqu'elles ont pour objet de détourner l'éditeur de la clientèle dudit concurrent (CA PARIS 4ch sect A 1er juillet 1991) ;
- le fait de dénoncer par voie de presse, des faits délictueux commis par des concurrents excède le droit de libre critique même si ces faits sont exacts (CA PARIS, 4ch sect 9 décembre 1992) ;
- l'article de presse portant sur le produit une appréciation générale très négative dépassant la libre critique et qui fait référence à l'appui de son appréciation à une enquête réalisée par un magazine de protection des consommateurs en laissant faussement penser que cette enquête concerne le produit en cause (Cass 2 ch civ, 8 avril 2004) ;
- la critique de la politique d'une société faite par une association sur son site Internet consistant à associer la marque de cette société à l'image de la mort (TGI PARIS 2ch 2 sec 9 juillet 2004) ;

- l'article publié dans une revue automobile qui met en cause gravement et sans référence à des études objectives et sérieuses les produits commercialisés par des distributeurs de pneumatiques (CA VERSAILLES 1ère ch. 1ere section 28 juin 1993) ;
- le rédacteur d'un guide gastronomique dispose d'une large liberté d'expression sous réserve que ses critiques soient entièrement dénuées d'un parti pris de dénigrement (TGI LYON, 18 mars 1994) ;
- L'utilisation par une entreprise d'un article critique à l'égard d'un concurrent publié dans une revue (Cass com 23 mars 1999).

Mais attention, la finalité du dénigrement qui consiste à jeter le discrédit sur un opérateur économique, concurrent ou non, sur ses produits ou ses services, le rapproche de la diffamation. Il est parfois difficile de savoir si le fait relève de l'une ou l'autre de ces qualifications. Toutefois, la Cour de cassation considère que l'action en concurrence déloyale pour dénigrement et l'action en diffamation sont exclusives l'une de l'autre.

Autrement dit, des appréciations même excessives touchant, les produits, les services ou les prestations d'une entreprise individuelle ou commerciale ne peuvent être qualifiées de diffamations dès lors qu'elles ne concernent pas la personne morale ou physique.

D. Focus sur la responsabilité du directeur de la publication

L'article 93-3 de la loi du 29 juillet 1982 indique que le directeur de la publication est responsable du délit de presse prévu par loi de 1881 comme auteur principal, lorsque le message incriminé a fait l'objet d'une fixation préalable et qu'à défaut l'auteur, et à défaut de l'auteur le producteur, sera poursuivi comme auteur principal.

L'article 27 de la loi du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet a cependant complété cet article en y ajoutant un alinéa ainsi rédigé :

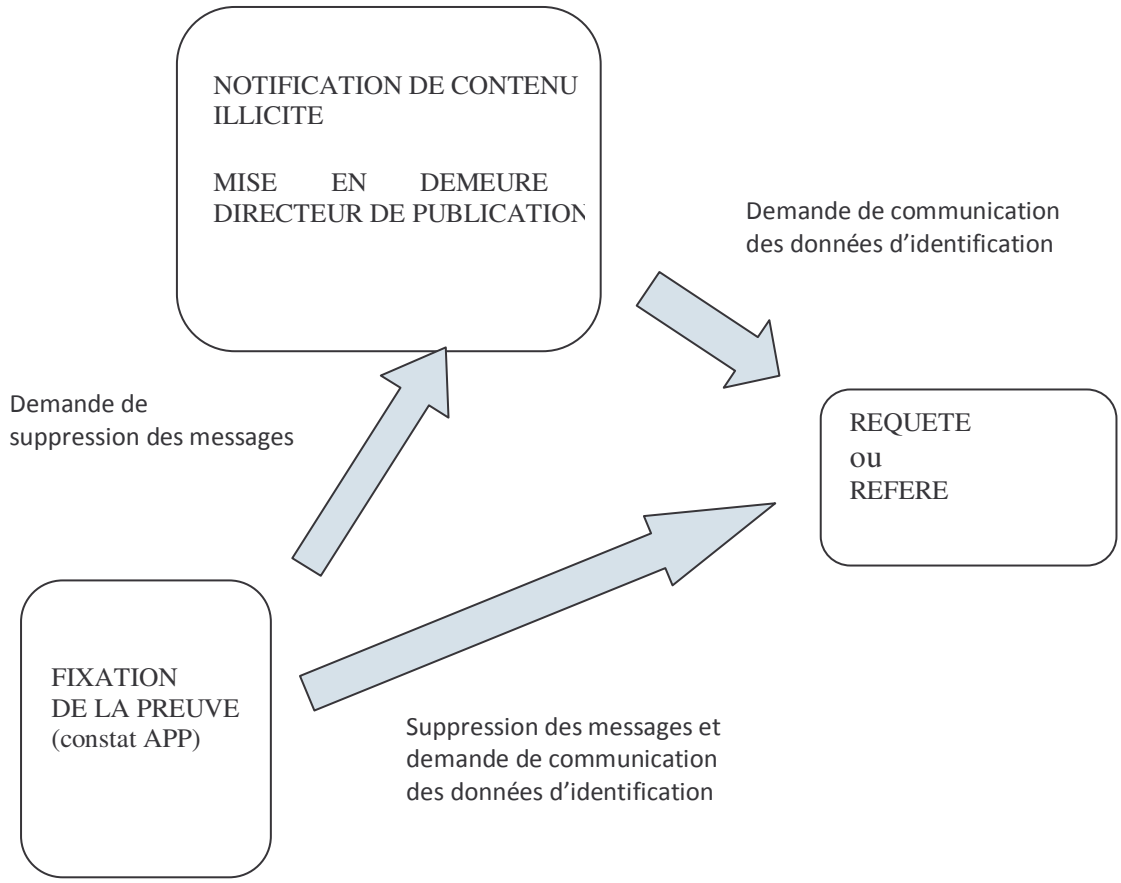
« lorsque l'infraction résulte du contenu d'un message adressé par un internaute à un service de communication au public en ligne émis par ce service à la disposition du public dans un espace de contribution personnel, identifié comme tel, le directeur ou le codirecteur de publication ne peut voir sa responsabilité pénale engagée comme auteur principal s'il est établi qu'il n'avait pas effectivement connaissance du message avant sa mise en ligne ou si dès le moment où il en eu connaissance il a agi promptement pour retirer ce message ».

Faute d'avoir été réservé aux seuls services de presse en ligne, cette disposition a vocation à s'appliquer indistinctement à l'ensemble des services de communication au public par voie électronique. Directement inspiré du régime juridique jusqu'à alors appliqué aux seuls services d'hébergement visés à l'article 6-I.2 et 3 de la loi du 21 juin 2004, la disposition nouvelle a manifestement entendu atténuer le régime de responsabilité des directeurs de communication s'agissant , comme l'a précisé le ministère de l culture lors des débats parlementaires (ASSEMBLEE NATIONALE/ 2ème séance jeudi 2 avril 2009) des « espaces dédiés à la libre expression des internautes tels que les forums et les blogs ».

Il en résulte qu'étant plus favorable aux directeurs de publication cette disposition leur est d'application immédiate, excluant en cela même que puisse être retenue à leur encontre une

complicité de délit de presse par aide ou fourniture de moyens quand ils peuvent se prévaloir de l'exonération découlant de la disposition nouvelle.

Enfin, bien que la modification introduite par la loi du 12 juin 2009 laisse prospérer la notion de « producteur » visée à alinéa 2 de l'art 93-3, directement inspirée de la communication audiovisuelle au sens strict et ne pouvant se concevoir en matière de communication en ligne que dans le respect des circonstances et des conditions qui en assureraient la justification pour la communication audiovisuelle dans son sens traditionnel- la responsabilité qui s'attache « au producteur » ne saurait à défaut de circonstances particulières peser systématiquement sur un directeur de publication qui se trouverait exonéré de sa responsabilité es qualité par application de la disposition nouvelle, sauf à vider de sa substance l'article 27 de la loi du 12 juin 2009.



CONCLUSIONS

Finalement, l'atteinte à la réputation diffamatoire, injurieuse, dénigrante fait appel à une parfaite connaissance juridique. Elle ne peut être engagée à la légère.

Derrière les outils de surveillance, il faut en fait des professionnels du droit pour qualifier les propos tenus sur la Toile car il ne faut pas oublier que l'objectif premier est de faire supprimer au plus vite ces propos malveillants.

V. Panorama des acteurs nationaux du marché de l'e-réputation

A. Typologie des acteurs du marché de la e-réputation

Source : Blog de Aref Jdey - http://www.demainlaveille.fr/

Le marché de prestataires en e-réputation se structure en 4 grandes catégories d'acteurs :

- Les éditeurs de logiciels payants (en orange sur la carte). Ce sont les acteurs les plus nombreux. Ils proposent des prestations au spectre plus ou moins large (collecte, veille - dont veille image et e-réputation- KM, analyse..). La dimension e-réputation est l'une des applications de leurs solutions ou au contraire leur cœur de métier.
- Les Pure players (en jaune) : ils sont spécialisés en veille image et e-réputation. Ils sont constitués d'agences de communication et d'éditeurs de logiciels. Ils sont pour la plupart de petite taille, dépassant rarement les 15 personnes.
- Les agences de communication et prestataires : ce sont des cabinets de conseil, des agences spécialisées en e-réputation ou les départements Internet de grandes agences de communication. La taille de ces prestataires est très variable. Ils fournissent des prestations d'analyse et de veille (sous forme de rapports) s'appuyant sur des logiciels développés en interne ou sur des solutions payantes plus complètes via un partenariat.
- Les applications gratuites : elles automatisent généralement une seule brique de la e-réputation ou surveillent un seul type de médias, rendant nécessaire un travail humain assez conséquent.

B. Guide des fournisseurs de solutions de veille et d'intelligence économique

L'univers de la veille & de l'intelligence économique et celui de l'e-réputation étant souvent très proche, il est possible de trouver des informations plus détaillées sur certains des acteurs présentés ci-dessus dans un guide spécifique réalisé par le groupe de travail « Intelligence économique et économie de la connaissance » du Groupement Français de l'Industrie de l'Information (GFII).

Le guide des fournisseurs de solutions de veille et d'intelligence économique présents en France répertorie les fournisseurs de solutions logicielles et fournisseurs de contenus proposant des fonctionnalités de veille et/ou d'analyse, ayant une activité commerciale en France. L'accès à ce guide a été facilité via la mise en place d'une base de données accessible librement sur le site Internet du GFII (***www.guideie.gfii.asso.fr***) et consultable en français et en anglais.

Cette initiative est le fait d'un mandat donné en 2008 par le Haut Responsable à l'Intelligence Economique pour mettre à jour le « Guide de recensement des outils de collecte, de traitement et de visualisation de l'information » réalisé en 2005 et publié par le Cigref en Janvier 2006.

Pour plus d'information sur les travaux

du Groupe Intelligence économique et économie de la connaissance du GFII,

vous pouvez contacter :

Ruth Martinez, Déléguée Générale du GFII

Tel 01 43 72 96 52

gfii@wanadoo.fr