Rumeur ou information ?

Information ou désinformation ?
Évaluer de manière critique les ressources issues de l'Internet

Texte : Pierre MÉRA
Révisions, résumés et intertitres : Pascal Pecquet (Université de Montpellier / Revue Cybergestion)
www.cyber-gestion.com

Publication : Revue Francophone de @management N° 08 mai 2003

Résumé : Évaluer les ressources du Net impose d'authentifier le nom de domaine, de tester la crédibilité du contenu… Néanmoins nombres d'entreprises hypothèquent leur capital confiance en laissant s'installer des campagnes de dénigrement, de saturation (mail bombing*) et surtout, elles négligent les sources multiples d'archivage de la rumeur. C'est vraiment jouer avec le feu !

Abstract : *Evaluating web resources requires authenticating the URL, testing content credibility… However, many firms put their trustworthiness at stake by ignoring defamation campaigns, mail bombings and they most especially neglect the various means of archiving rumors. Now that's playing with fire !*

(*) Les mots-clés de la cybergestion sont sur www.cyber-gestion.com à la rubrique Dictionnaire.

Relativement épargné au départ du fait de son faible taux de connexion à l'Internet, le monde éducatif se trouve désormais confronté, comme tout le monde, à l'arrivée des hoax, ces messages qui colportent des canulars, des rumeurs, des virus plus ou moins dangereux…

Avec le déploiement de l'ADSL, de plus en plus nombreux sont en effet les établissements d'enseignement à proposer, aux élèves comme aux étudiants, des adresses électroniques individuelles sur un sous-domaine de leur académie. Résultat : malgré des filtres en plate-forme centrale, ces boîtes sont rapidement la cible du spam et les enfants peuvent donc trouver toutes sortes de messages dans leur courrier…

Ce qui fera peut-être sourire un adulte peut s'avérer bien moins anodin lorsqu'il s'agit d'enfants, ou de jeunes adultes, tout simplement parce que ceux-ci ne possèdent pas nécessairement les clés de décryptage et que, d'autre part, ils se trouvent sous le couvert d'un lieu qui se veut garantir par essence la crédibilité des informations transmises. La vigilance sur la valeur de l'information y est donc, a priori, faible.

Dans tout ce courrier indésirable, les hoax possèdent un statut particulier car ils sont le véhicule d'informations volontairement trompeuses. S'il peut s'agir parfois de canulars sans grandes conséquences (**Raffarin 500mg**) ou d'alertes imbéciles aux faux virus (**Sulfnbk** etc.), ce sont aussi des rumeurs malveillantes (**Pentagone**) susceptibles d'abuser jeunes et moins jeunes (voir le site http://www.hoaxbuster.com/ pour une liste de hoax

Et la force du hoax est encore accrue par le fait qu'il vous est transmis bien souvent par l'un de vos correspondants, croyant de bonne foi faire oeuvre utile. Les effets de groupe chez les jeunes accélèrent ainsi la propagation des rumeurs…

On comprend dès lors pourquoi l'École ne peut pas rester indifférente sur cette question. En tant qu'institution à qui les enfants sont confiés, **elle se doit de contrôler ou de valider l'information qui leur est délivrée,** quel qu'en soit le canal. C'est ainsi que de nombreuses entreprises ont senti l'émergence d'un marché et proposent aux établissements des systèmes de filtrage coûteux en jouant assez facilement sur les peurs diffuses que suscite Internet. Sur ce point au moins, la rumeur a fait son effet !

La problématique de l'École n'est évidemment pas la même que celle de l'entreprise. Virus, chevaux de Troie, spam, attaques… menacent gravement la sécurité des données des entreprises et consomment du temps de travail. À quelques exceptions près (données administratives, dossiers d'élèves en classes post-bac…), ce ne sont pas des problèmes cruciaux pour le monde éducatif. Notre problème est bien davantage celui de la crédibilité et de la valeur de l'information transmise, puisque notre « fonds de commerce », c'est la connaissance !

À l'intérieur de l'Éducation Nationale, l'académie de Grenoble a mis au point un firewall basé sur Linux, SLIS, repris par plusieurs autres académies et qui possède également un module de filtrage fondé sur SquidGuard.

Pourtant, tous ceux qui fréquentent un tant soit peu les réseaux informatiques savent que ce sont là de bien fragiles protections. **Et ce d'autant plus que ces systèmes ne filtrent en général pas les hoax puisqu'ils ne filtrent pas le spam en tant que tel !** Il nous semble donc doublement absurde de se cacher derrière ces hypothétiques barrières. D'une part parce que, comme toutes murailles, elles seront abattues, et ce d'autant plus facilement que rares sont les établissements disposant de personnes-ressources capables de suivre le rythme des patchs de protection et de correction. Et d'autre part - c'est l'essentiel - parce que la mission de l'École est avant tout éducative : sa vocation n'est pas d'élever de hauts murs mais de conduire ses élèves à un minimum de discernement et d'autonomie… ! L'éveil de l'esprit critique, la mise en œuvre d'un doute méthodique sont bien des objectifs pédagogiques.

Malheureusement, la formation encore très sommaire des enseignants aux réalités d'Internet rend les choses assez difficiles au quotidien.

L'objectif, aussi bien pour les personnels que pour les élèves ou les étudiants, est donc bien la formation ! Ce qui permettrait, au passage, qu'aussi bien dans leur vie privée que dans leur vie professionnelle, les futurs adultes aient une attitude active concernant la sécurité ! Cependant, l'Éducation Nationale n'échappe pas à cette règle étrange qui permet de toujours trouver de l'argent pour financer des systèmes (serveur + firewall par exemple) et bien peu pour assurer la formation.

Malgré tout, de nombreux travaux ont déjà été entrepris pour aider les élèves (et les enseignants) à analyser les sites web. La figure n° 1 présente une première webographie de sites proposant une démarche. À cet égard les Canadiens et les Belges font figure de pionniers. En France, c'est le Clémi (Centre de Liaison de l'Enseignement et des Moyens d'Information) qui dépend du Centre National de Documentation Pédagogique (CNDP) qui s'est penché sur la question.

I. Déployer une méthode d'investigation des ressources du Web

Une réalisation importante a ainsi été le projet Educaunet. Les groupes académiques aussi s'intéressent également à la question comme en témoignent, par exemple, les pages consacrées à la validation de l'information sur le site de l'Académie de Versailles. Ces pages sont à la fois une réponse argumentée à une rumeur (!) et une tentative méthodologique :

- la rumeur est celle qui circule de façon persistante au sein du monde éducatif et qui consiste à laisser croire qu'Internet constitue une zone de non-droit où les enfants seraient en danger. Cette rumeur est relayée tout aussi bien de façon externe par les « marchands de sécurité », que de façon interne par une partie de la hiérarchie qui voit d'un mauvais œil cet espace de connaissances peu ordonnées qui échappe à son contrôle. Soigneusement entretenue, la rumeur justifie alors le rejet en bloc de l'accès à Internet et valide l'inquiétude des enseignants vis-à-vis d'un média dont ils n'ont pas toujours les clés.
  Face à cette approche peu rationnelle, nous tentons de montrer que cette prévention devant Internet est avant tout due à une méconnaissance de ce qu'est ce réseau des réseaux. En connaître la mécanique c'est, évidemment, prendre la mesure des « risques ».
- dans un deuxième temps, nous proposons une méthode de travail pour effectuer une recherche d'informations et en valider les résultats. À partir d'un exemple (la recherche du texte de la loi Gayssot sur le racisme) nous montrons que la validation de l'information nécessite une véritable démarche, qui doit être systématique.

Ressources	Sites	Commentaires
Comment évaluer les ressources d'un site	Fédération de l'Enseignement Secondaire Catholique Belge http://users.skynet.be/ameurant/francinfo/validite/index.html	Un site remarquable car il propose une méthode très complète avec de nombreux exemples et documents utiles. On y trouve notamment la présentation détaillée d'un site consacré à Martin Luther-King qui dissimule des propos violemment racistes.

J'évalue un site Web / une page Web	École de bibliothéconomie et des sciences de l'information http://www.ebsi.umontreal.ca/jetrouve/internet/evalsite.htm http://www.ebsi.umontreal.ca/jetrouve/internet/evalpage.htm	Une grille toute prête pour aider les élèves à évaluer un site. Faculté des Arts et des Sciences. Université de Montréal.
Apprendre à lire une adresse de site	Centre de Liaison de l'Enseignement et des Moyens d'Information) Ministère de l'Éducation Nationale http://www.clemi.org/formation/fiches/fiche22.html	Une fiche pédagogique pratique
La crédibilité des informations sur le WEB	Unité Technologies de Formation et Apprentissage (Tecfa) - Faculté de Psychologie et des Sciences de l'Éducation de l'Université de Genève http://tecfa.unige.ch/themes/FAQ-FL/credibilite_info_web/credibilite_info_web.html	Une page simple qui pose les questions essentielles, notamment en ce qui concerne le but poursuivi par ceux qui mettent de l'information en ligne. Une seconde page propose un exemple
Grille d'évaluation d'un site Web	Auteur : Robert Bibeau, Ministère de l'Éducation du Québec http://ntic.org/guider/textes/div/bibgrille.html	Une grille d'évaluation immédiatement utilisable fournie avec une notice explicative.
Fig. n° 1 : Des ressources pour apprécier le contenu d'un site.		

Tous ces dispositifs visent à ce que chaque utilisateur d'Internet puisse mettre en œuvre, systématiquement, une méthode qui lui permette d'évaluer, par lui-même, la valeur de l'information qu'il rencontre ou qu'on lui propose. Plus l'utilisateur est jeune, plus la démarche est difficile puisqu'il s'agit essentiellement de repérer des indices et de les confronter à ce qu'on sait par ailleurs.

Prenons trois exemples pour expliquer cette démarche.

I.1. Pour authentifier le nom de domaine ?

La recherche d'informations sur la présidence de la république peut conduire notamment à deux sites : www.elysee.fr d'une part et www.elysee.org d'autre part.

Le second de ces sites est une parodie, en ligne depuis plusieurs années. L'analogie graphique entre les deux sites était bien plus forte dans les débuts. La supercherie va sauter aux yeux de quiconque possède un peu de sens critique. C'est pourtant loin d'être évident pour les plus jeunes, pour lesquels il existe une sorte d'autorité intrinsèque de la chose écrite, surtout si celle-ci apparaît sur un écran… comme à la télé ! Toutefois, la figure n° 2 présente une séquence de validation qui conduira à tester le contenu disponible du site.

Une séquence de travail sur ces deux sites portera sur :

- l'étude du TLD (Top Level Domain) des deux sites, en l'occurrence .fr ou .org. Les utilisateurs doivent être sensibilisés à l'importance de ces TLD comme élément de crédibilité de l'émetteur de l'information : disposer d'un TLD en .fr ne constitue pas un brevet d'honorabilité et de crédibilité, mais garantit que l'émetteur s'impose de respecter les lois françaises en matière de diffusion de l'information, lesquelles sont assez strictes, notamment pour la diffusion de fausses nouvelles… ! Celui qui va rechercher un TLD en .tv, en revanche, a peut-être quelque chose à dissimuler…
- la recherche de l'auteur de la page. Deux indices ici permettent de douter : d'une part la page d'accueil est signée « Les amis du président de la République » ; d'autre part la page affiche un logo « Web indépendant ». Difficile d'imaginer qu'on se trouve sur un site officiel. Mais le site officiel, www.elysee.fr, ne fournit lui-même guère d'informations positives : on peut écrire à un webmestre et on dispose de l'adresse postale de la présidence. On ne trouve pas d'indication d'un directeur de la publication, ni d'un numéro de téléphone qui permettrait de vérifier l'authenticité du site.
- la cohérence des éléments proposés. La « citation » chiraquienne, quand bien même serait-elle authentique (!), est peu probable sur un site institutionnel…
- la fraîcheur de l'information : le site elysee.org n'a apparemment pas bougé depuis 1997 ! Ce n'est évidemment pas le cas du site officiel qui est à jour.

L'accumulation des indices permet de déterminer sans trop de risque de se tromper lequel des deux est le vrai site de la Présidence. L'exemple proposé ici est simple. Le second pose un problème plus délicat.

I.2. Pour valider le contenu d'un site ?

Certaines informations ne se trouvent que sur des sites étrangers. Ainsi, pour disposer d'informations de première main sur la politique économique du gouvernement américain, peut-il s'avérer pratique de rechercher le site de la Maison-Blanche. Cette fois, on trouvera quatre sites possibles :

Sites	Contenu disponible	Indices trouvés
www.whitehouse.gov	Le site officiel	Le TLD en.gov n'est autorisé que pour des sites officiels ; actualité du site ; richesse du contenu multimédia (= gros moyens financiers) ; contacts multiples.
www.whitehouse.com	Site pornographique	Avertissement légal Références nombreuses à l'aspect « adulte » du site.
www.whitehouse.net	Quelques fausses informations, parodies	Austérité de la mise en page pour un site officiel ; pas de date de mise à jour, pas d'agenda ; renvois au site officiel ; aveu de parodie sur une page ; pauvreté du contenu ; mais attention : quelques liens renvoient à des pages du site officiel, accentuant la confusion !
www.whitehouse.org	Contenu parodique multiple	Les photos de Une (à défaut de comprendre tous les textes) devraient permettre de s'interroger ; une page indique clairement qu'il s'agit d'une parodie.

Fig. n° 2 : La séquence de validation du contenu disponible.

Dès lors que l'utilisateur s'avère peu compétent en anglais, comment saura-t-il lequel de ces sites est « le bon », et ce d'autant que le site www.whitehouse.org est d'excellente facture graphique. Si on ne l'a pas averti de l'importance des suffixes, il aura du mal à déterminer d'emblée quel est le site officiel, même si Google place opportunément le site www.whitehouse.gov en tête de liste.

Seul le site www.whitehouse.org indique discrètement en bas de première page qu'il s'agit d'une parodie. Et ne parlons même pas du site en suffixe .com qui renvoie carrément à des pages pornographiques (Google le laisse tout de même supposer).

On voit comment il peut être relativement facile d'abuser un utilisateur trop pressé, peu attentif ou insuffisamment compétent. Lequel colportera ensuite comme « officielles », des informations trouvées sur un site qui est au mieux parodique, au pire un lieu de désinformation ou de dénigrement !

I.3. Pour tester la crédibilité de l'information !

Les deux exemples précédents portent sur des informations recherchées et trouvées par l'utilisateur. Mais qu'en est-il lorsque l'utilisateur reçoit un message qu'il n'a pas sollicité, qui l'alerte sur une menace ou lui propose une information fortement « confidentielle » ?

Masqué derrière l'apparente crédibilité que lui confère l'expéditeur qui est en général un correspondant connu du récepteur, le hoax[1] prend toutes les apparences d'une information véritable. Et ce d'autant plus que la menace annoncée (ou l'espérance de gain) est plus importante ! Ce n'est pas pour rien que les rumeurs les plus folles courent en période de crise grave (pendant les guerres par exemple).

Ainsi, par exemple, ce message (sujet 7, p. 41 de ce PDF) concernant les additifs alimentaires, voit sa crédibilité renforcée par le climat d'insécurité alimentaire que nous connaissions en 2000-2001. Alertée sur le sujet et inquiète, l'opinion accepte d'autant plus et de façon un peu masochiste tout élément susceptible de conforter le sentiment général (c'est le : « on vous l'avait bien dit ! »).

L'analyse de ce texte montre combien l'auteur a employé des « effets de réel », c'est-à-dire toutes sortes de procédés qui conduisent à baisser la garde :

- une source scientifique apparemment incontestable
- une astuce rhétorique appelant le lecteur à « vérifier » l'info. Ce qu'on ne fait jamais naturellement !
- une typologie pseudo-scientifique et un vocabulaire médical qui renforcent le sentiment d'authenticité (l'autorité de la blouse blanche, bien connue des publicités pour dentifrices !)
- une dramatisation inquiétante qui atténue la vigilance (face à une telle menace, il y a urgence !)
- la révélation d'un complot ! (on nous cache quelque chose et la vérité est ailleurs)…

Dans certains cas, les messages s'appuieront sur une forte ressemblance avec des documents authentiques (voir par exemple les virus transmis dans des messages d'apparence Microsoft !), d'autres insisteront sur l'urgence de la situation…

Notre travail consiste donc à révéler les « trucs » employés dans ces messages, de façon à prévenir l'utilisateur de ce qu'il peut rencontrer le plus couramment, et ainsi le conduire à prendre du recul vis-à-vis des messages reçus, tout spécialement lorsque ceux-ci font référence à des situations dramatiques : enfants enlevés, virus destructeurs, pollutions extrêmes…

Comme on espère l'avoir montré ici rapidement, aucune barrière ne pourra remplacer la formation de l'esprit critique de l'utilisateur. Celui-ci est mis à mal parce qu'Internet est souvent un univers de communication dont il maîtrise peu les codes. Dès lors, difficile de faire la part des choses entre ce qui est rationnel et ce qui ne l'est pas !

Seul un vrai travail de formation, précis et suivi, peut permettre à chacun des utilisateurs de valider l'information dont il prend connaissance sur Internet et de ne pas rediffuser bêtement tous les bruits qu'Internet propage et amplifie. Il est clair que cette formation a également des incidences sociales et politiques en rendant le citoyen plus critique dans ses analyses quotidiennes et, peut-être, moins sensible aux charmes de l'irrationnel…

II. Des entreprises qui hypothèquent leur capital confiance

En ce qui concerne les entreprises, les attaques ont une portée toute différente. C'est tout le capital de confiance vis-à-vis de la marque ou de la société qui peut se voir balayé en peu de temps.

À cet égard, Internet représente une caisse de résonance remarquable et surtout un formidable vecteur de continuité de la rumeur. Plusieurs années après, celle-ci continue à circuler au travers des moteurs de recherche, des archives de forum, de pages web obsolètes mais toujours accessibles… Et peut donc retrouver brusquement une actualité.

[1] Hoax = canular diffusé par voie informatique.

La malveillance mais aussi la guerre économique sont à l'origine de ces attaques qui n'ont évidemment pas attendu Internet. Ainsi, par exemple, on se souvient de Perrier, accusé en janvier 1990 d'avoir commercialisé des bouteilles contenant des traces de benzène. Il ne s'agissait pas d'une rumeur ! Perrier a confirmé. Et a dû, dans la foulée, retirer 160 millions de bouteilles, non pas parce que la santé des consommateurs était en jeu, mais bien à cause de la menace qui pesait sur son image. Il a fallu 10 ans à la firme, après bien des péripéties (dont le licenciement de la moitié de ses effectifs), pour renouer avec les bénéfices.

Aucun rapport avec Internet ? Pas si sûr ! Lorsqu'en juin 1999, la société Coca-Cola dut retirer en Belgique puis en France plusieurs millions de canettes de Coca, de Sprite, de Fanta… suite à des malaises répétés de consommateurs et sous la pression des autorités sanitaires, Internet n'était pas encore, en Europe, le réseau grand public qu'il est en passe de devenir. Pourtant, déjà, de très nombreux sites et forums gardent trace de cet événement. Et quel rapprochement effectue aussitôt certains d'entre eux ? Perrier évidemment ! Ainsi à dix ans d'intervalle, le Réseau remet au jour (modestement il est vrai), une « actualité » qu'on croyait « passée ».

Dès lors on comprend qu'il est essentiel pour les entreprises, soit en direct si elles en ont les moyens, soit par l'intermédiaire de cabinets spécialisés, d'assurer une veille « informationnelle » sur l'Internet (web et forums principalement) et de réfléchir à une communication de crise adaptée.

II.1. ...Par le parasitage du nom de domaine :

Le cyber squatting consiste à acheter un domaine au nom de l'entreprise sur un TLD particulier ; domaine que l'entreprise n'a pas songé à s'approprier : .biz, .tv, .org, .net. Cette pratique, courante dans les débuts de l'Internet grand public (il y a seulement 5 ans !) est tombée en désuétude au fur et à mesure que des textes plus contraignants ont été adoptés par les États et par l'ICANN (textes de 1999), notamment pour imposer le respect de la propriété industrielle.

Ainsi, France 2 et France 3 ont été victimes de ces pratiques en France, Tractebel en Belgique…

Aujourd'hui encore, il serait possible de squatter un domaine, en utilisant le TLD d'un État peu regardant par exemple. La réponse de l'entreprise ne peut guère être que juridique, sans assurance de succès, puisqu'à la base de la répartition des noms de domaine on trouve la clause premier arrivé / premier servi. Une vigilance en amont, notamment au fur et à mesure que sont mis en service de nouveaux TLD (récemment les .biz, .info…), est donc nécessaire.

II.2. ...Suite à des campagnes de dénigrement :

Le dénigrement peut être la conséquence du cas précédent dès lors que le site entreprend une campagne contre la marque par exemple. Mais l'action peut provenir aussi bien de forums, de listes de diffusions, que de sites web. À cet égard, on peut se souvenir de la campagne contre Danone suite aux licenciements chez LU. Danone a bien obtenu la condamnation du site jeboycottedanone, mais pas du fait de l'appel au boycott de ses produits.

En effet, c'est pour l'usage illicite du nom de la marque et de son logo (atteinte à la propriété industrielle) que le site a été condamné. Il n'est pourtant pas certain que l'objectif ait été atteint par l'entreprise : la communauté des internautes, très choquée par la brutalité du procédé, dans ce qui était perçu comme une réponse économique et politique (le boycott) à une agression (les licenciements), s'est aussitôt fait largement écho du jugement. La presse écrite s'en est mêlée, un nouveau site - mieux armé - a pris le relais du boycott… Tout cela a contribué notablement à la chute d'image de Danone, notamment son image sociale, pour le rétablissement de laquelle Franck Riboud a dû batailler ferme dans les médias.

On retrouve une situation analogue dans le cas de la société pere-noel.fr, accusée par plusieurs sites de ne pas livrer ses clients, de débiter leurs comptes de sommes indues etc. À un détail près : la notoriété initiale de l'entreprise était inexistante. Elle avait donc moins à perdre.

La société a fait condamner pour diffamation les auteurs du site defense-consommateur.com en mai 2002. Mais… les ex-dirigeants de la société (les frères Fur) sont eux-mêmes jugés au pénal en mai 2003, pour de nombreuses malversations présumées. Là encore, le « remède » a été pire que le mal : l'action menée par la société a mobilisé les internautes. Les auteurs du site ont réuni 40 000 signatures, déclenchés des enquêtes d'organismes officiels, dont la DGCCRF (Direction Générale de la Concurrence, de la Consommation et de la Répression des fraudes).

On voit bien là l'effet boule de neige de la transmission de l'information sur Internet, lié notamment au caractère parfois fortement « communautaire » du réseau : des groupes militants

s'organisent et se mobilisent très rapidement en utilisant tous les canaux à leur disposition (mél, forum, chat, web), avec des conséquences inéluctables : déformation des faits initiaux, multiplications des rumeurs… Il devient quasiment impossible d'y remédier.

II.3. ...À l'issue d'une campagne de saturation :

Le mail-bombing est une technique récente qui vise à encombrer le réseau. L'actualité récente nous en offre un exemple frappant. À partir du 13 mai 2003, plus de 80 000 courriels ont été adressés aux principaux leaders syndicaux (FO, CFDT, CGT) par des militants d'une fraction de l'UMP, submergeant les serveurs des organisations syndicales en question.

Afin de tenter de se protéger de possibles suites judiciaires, les militants de la fraction en question, la Droite Libre, n'ont pas procédé eux-mêmes, mais encouragé leurs adhérents à adresser chacun un message de protestation aux leaders en question.

Si cette action est mentionnée ici, c'est essentiellement du fait du retentissement médiatique qu'elle a pu avoir. C'était en effet la première fois qu'une attaque électronique était utilisée publiquement à des fins politiques en France.

Les entreprises peuvent aussi être prises pour cible par ces campagnes de saturation. Mais il est clair que les conséquences, surtout « matérielles » (blocage d'une partie de l'activité électronique de l'entreprise), sont sans commune mesure avec les attaques contre la réputation de la société.

II.4. ...En négligeant les sources multiples d'archivage de la rumeur :

Les hoax sont certainement les menaces les plus dangereuses, notamment parce qu'il est extrêmement difficile d'en cerner la source et par la suite de s'en défendre. Face à une rumeur qui circule, l'entreprise se situe toujours en réaction. Elle n'a pas l'initiative. Et le moindre faux pas peut accroître le mal comme on a pu l'apercevoir plus haut.

À cet égard, on peut citer trois cas. Les deux premiers sont antérieurs à Internet, mais plusieurs sites reprennent aujourd'hui l'information, ne serait-ce que pour la contester…

- ·En premier lieu, la société **Pepsi** qui en 1993 fut accusée d'avoir commercialisé des cannettes contenant des seringues et divers autres objets. Largement relayée par les médias, la rumeur conduisit à une baisse de chiffre d'affaires de 25 millions de dollars.
- Autre cas intéressant, celui de la société **Poilâne,** accusée depuis 1993 de financer l'extrême droite. La rumeur trouve son origine dans le livre d'une journaliste qui est allée un peu vite en besogne. Et « l'information » a été reprise maintes fois et démentie à plusieurs reprises publiquement par ceux-là même qui avaient pu la relayer. Elle a pourtant retrouvé toute son actualité au moment de la mort du boulanger, en novembre 2002, lorsque le magazine du Front National, National Hebdo, lui a rendu un hommage appuyé en titrant « Adieu à l'un des nôtres… ». Et « l'information » a été reprise par le journal Libération ! Rien d'étonnant, donc, que depuis, de nombreux sites sur le Web répandent l'accusation en s'interrogeant sur son bien fondé. L'entreprise n'est pas vraiment menacée par cette rumeur persistante et a choisi de ne pas y répondre. Celle-ci jette cependant un voile sur son honorabilité et constitue une épée de Damoclès : nul ne peut prévoir si un événement quelconque, éventuellement étranger à l'entreprise elle-même, ne pourrait pas soudain redonner à la rumeur une vitalité nouvelle avec des conséquences imprévisibles.
- Plus récemment, on peut également citer le cas de la société des **Champagnes Veuve Clicquot,** victime d'un hoax par courrier électronique annonçant l'envoi gratuit de six bouteilles à celui qui adresserait ledit courrier à dix nouveaux destinataires avec copie à l'entreprise. Il s'agissait, prétendait-on, d'élargir le fichier client de la société. La rumeur trouvait là une forme de crédibilité, dans la mesure où les systèmes de parrainages sont fréquemment employés par les entreprises, avec cadeaux à la clé. Veuve Clicquot a ainsi commencé à recevoir des centaines de courriers réclamant la récompense promise ! L'entreprise a communiqué sur le sujet dans la presse et placé un démenti sur son site. Là encore, les conséquences immédiates sont peu importantes et l'enjeu reste purement commercial. La réputation de la marque n'est pas réellement atteinte. Mais il persistera longtemps un doute… nourri en partie par les sites qui font écho à l'événement, quand bien même ils le démentent !

Cette caractéristique d'Internet doit être mesurée par les entreprises qui cherchent à réagir : Internet n'est pas seulement un média de l'instant. C'est aussi une archive impitoyable, à la mémoire longue !

II.5 En jouant avec le feu

Le marketing étant toujours à l'affût des modes, rien d'étonnant à ce que certains aient trouvé un charme fou dans le mode de propagation des rumeurs sur Internet : un bouche-à-oreille ultrarapide et ultra-performant. Pourquoi alors ne pas l'utiliser à des fins positives pour l'entreprise ? C'est ainsi que naît le marketing viral, un concept qui consiste, dans certains cas, à lancer des rumeurs accrocheuses puis à compter sur cet appât pour attirer un public cible bien particulier qui sera lui-même, notamment par son courrier électronique, le vecteur bénévole de cette nouvelle forme de publicité. Ainsi la marque Diesel se vante d'avoir créé de toutes pièces une fausse star de la chanson ; le « Projet Blair Witch », film d'angoisse à petit budget, obtient un succès planétaire grâce à des rumeurs savamment distillées dans les forums, et à de « faux » sites webs apportant de prétendues informations inédites.

Mais attention, là encore Internet est un média très différent de ceux qui sont utilisés habituellement par les annonceurs. On imagine difficilement le public réagir à une campagne d'affichage par une contre-campagne ou bien financer un contre-spot télé. Sur Internet, c'est possible ! Total s'en souvient encore et s'en souviendra longtemps, comme en témoignent les sites qui reproduisent encore aujourd'hui, les affiches de contre-publicité créées suite à la marée noire de l'Erika et largement reprise dans les médias institutionnels ! « Nous avons juridiquement raison mais médiatiquement tort », déclarait, maladroitement d'ailleurs, Michel Delaborde, dircom de TOTALFINA.

Internet est un outil de communication. Mais, pour une fois, il est à double tranchant !

Il y a donc un risque réel à utiliser sans « conscience » les principes du marketing viral. Un faux pas d'une part, et il y a des chances que l'entreprise subisse un contrecoup qu'elle aura du mal à stopper. Et d'autre part, diffuser des rumeurs sur Internet, cela s'apparente à crier au loup. Le jour où l'entreprise sera à son tour victime de la rumeur, qui pourra croire ses démentis ?

Au final, nous sommes face à deux exigences très différentes :

- le monde éducatif doit préparer les jeunes à s'interroger sur les informations qu'ils reçoivent et à mieux connaître leurs canaux de diffusion. L'acquisition d'un réflexe critique chez chacun est importante mais il est bien évident que cela n'empêchera pas les rumeurs de se répandre...
- l'entreprise gagnera à disposer de personnels alertés sur la question de la rumeur. Mais il est clair que sa problématique prioritaire est celle de la réponse à apporter. À la lumière des quelques exemples présentés ici, on peut sans doute retenir au moins deux choses : d'une part les méthodes de la communication de crise « traditionnelle » ne sont peut-être pas nécessairement efficaces lorsque la rumeur vient d'Internet, notamment parce que les Internautes sont « autonomes » par rapport à l'information. D'autre part, il convient de garder à l'esprit que tout ce qui a été écrit restera longtemps et d'accès quasi instantané. Grâce aux moteurs de recherche, une communication inappropriée pourrait tout aussi bien se retourner contre l'entreprise au moment où celle-ci s'y attend le moins… !

Pierre Méra
2003

Source : http://www2.presse.ac-versailles.fr/Pedago/Rumeur09.htm