MANIPULATION À DISTANCE ET FASCINATION CURIEUSE

Les pièges liés au spam

Nicolas AURAY

DOI: 10.3917/res.171.0103

Les technologies de l'information et de la communication ont haussé la quantité globale d'information qui nous arrivent (Shapiro et Varian, 1999), nous insérant dans des écologies informationnelles denses (Licoppe, 2009) et générant une saturation cognitive. Un point central est qu'elles ont développé une situation d'incertitude ou d'insécurité cognitive, du fait de l'ignorance sur la source de l'information. À côté des témoignages venus de proches, où l'information est enchâssée dans une structure d'interconnaissance interpersonnelle qui permet d'en garantir la crédibilité, à côté également des médias de masse qui offrent une information vérifiée ou certifiée, voire officielle, émergent des canaux de communication transversaux ou horizontaux par lesquels arrivent des informations non garanties, surprenantes mais officieuses (Gensollen, 2006), et susceptibles de poser des problèmes de confiance. Notamment, Internet est une caisse de résonance pour la circulation d'histoires urbaines ou de chaînes proliférantes (Heiderich, 2004). C'est en effet un trait qui définit la rumeur, le « bruit qui court », de ne pas émaner de source certifiée ou déterminée (Kapferer, 1998). Internet a ainsi pu être qualifié de formidable amplificateur de rumeurs (Froissart, 2007). Un peu dans la filiation de l'article de Marc Bloch sur les fausses nouvelles de la guerre, où il était mis en évidence que, dans un contexte d'isolement entre les personnes (comme des soldats obligés de rester dans leurs tranchées), la vulnérabilité à la rumeur augmentait, de nombreux travaux ont mis en évidence, lorsque les individus ne sont pas reliés par des réseaux interpersonnels mais relaient l'information sans se connaître par le biais des routeurs de l'Internet, que le risque de vulnérabilité aux rumeurs et leur circulation augmentent fortement [1].

Ce couplage entre le caractère surprenant des énoncés qui circulent, conférant ainsi de l'agrément au fait de les répéter ou de les croire, et l'absence de procédures simples et claires pour déterminer leur fiabilité, génère une *vulnérabilité* des récepteurs, un affaiblissement de leur résistance critique, une

1. Pour une vue récente – et orientée – de l'Internet comme « amplificateur de rumeurs conspirationnistes », cf. Corcuff (2010).

difficulté à réguler l'excitation curieuse[2]. Du fait de la difficulté d'exercer sur un tel univers marqué par la déterritorialisation le monopole de la violence légitime, Internet est par ailleurs fortement ouvert aux illégalismes et aux tentatives d'escroquerie, comme le montre l'exemple de la prévalence du « spam », l'envoi de courrier non sollicité reposant sur la récupération illicite de l'adresse mail du destinataire[3] ; l'insécurité d'un tel monde est lié au fait que l'escroc, le manipulateur de cadre (le spammeur), a toujours un temps d'avance sur les techniques de protection contre lui (les logiciels antispam).

Une telle insécurité ne peut être compensée que par l'acquisition de compétences individuelles permettant à chacun de se protéger : la capacité à savoir lire un champ d'en-tête de mail, à recouper des informations étonnantes en utilisant des moteurs de recherche ; autant de savoir-faire minimaux qui sont à l'origine de l'institution d'un « passeport de compétence », le b2i, en France, depuis 2006. Or, avec la diffusion du haut débit et la résorption progressive de la fracture numérique sur le plan des équipements, une part quantitativement de plus en plus importante de « l'audience » de l'Internet est constituée par de nouveaux utilisateurs, plus âgés et moins diplômés, peu investis par la maîtrise de ces outils (voire réfractaires à ceux-ci), qui se sont mis à Internet essentiellement à des fins pratiques (pour payer ses impôts, recevoir les photos de ses petits-enfants ou faire son billet de train), ou par obligation (afin d'exercer leur activité professionnelle). C'est précisément pour ce public très large de réticents, de réfractaires, que l'usage d'Internet suscite des risques et des insécurités, qui se traduisent par la convergence de cette population sur deux attitudes culturelles prééminentes : une attitude de *crédulité*, quant aux mails reçus ou aux informations lues sur des sites, au sens d'une disposition à tenir trop facilement pour vraie une proposition communiquée par autrui sans soumettre la véridicité de l'information transmise à une procédure rationnelle (Clément 2005) ; une attitude, par réaction, de *scepticisme radical*, qui consiste, sur le modèle d'une crédulité inversée, à refuser systématiquement tout appui sur ces sources d'information. Dans les deux cas se produit un dérèglement du « filtre cognitif », ce dispositif intérieur de jugement permettant l'évaluation et le tri entre les informations venues d'autrui.

---

2. Les « technologies de l'Internet » – la fonction « *j'ai de la chance* » de Google, les recommandations insolites des sites de folksonomy, l'affichage de « ceux qui vous font rêver » sur les sites de rencontre en ligne – ont répandu une figure du butinage, de la trouvaille heureuse et de la cueillette, qui dit à la fois une *profusion*, un foisonnement, et une *immédiateté* de biens offerts à la prise, comme tombant tout cuits sous la main. Cf. Auray (2010).

3. D'après le rapport mensuel de l'entreprise Symantec, 90,7 % en 2007. Dont 85 % envoyés par des botnets.

La recherche ici présentée, à caractère exploratoire, vise à documenter, à partir de 12 cas de « manipulation de cadre » (Goffman 1991) utilisant le canal du mail, le cheminement de victimes sous l'emprise d'une relation d'escroquerie par Internet (fausses promesses de gains ou romance par scam). La caractéristique de ces relations d'escroquerie est de découler systématiquement de l'envoi massif de courriers non sollicités, autrement appelés « spams », afin d'hameçonner des jobards. Ainsi, l'opposition entre « spam » et « scam » est surtout une différence de construction : le spam fait surtout référence à la phase d'élaboration du mail d'hameçonnage et à la constitution de gigantesques bases d'adresses, le scam en revanche s'intéresse à l'entretien, postérieur au hameçonnage, d'une relation dyadique avec une victime. Nous avons réalisé 12 entretiens avec d'anciennes victimes de « scam » sur le mode d'entretiens biographiques « d'après coup », c'est-à-dire après « l'éveil » des victimes à la fraude, entre 2008 et 2010. Les victimes ont été identifiées à partir de contacts avec la principale association francophone de lutte contre ces fraudes[4]. Elles se décomposent en trois groupes de taille égale (trois interviews) : 1) des victimes de « spam » à but commercial, i.e. d'escroqueries ayant pour but de forcer l'achat de particuliers pour des produits licites ou illicites mais à haute désirabilité : des poudres de Perlimpinpin, des élargisseurs de pénis, des élixirs de jouvence, des roues de la fortune ; 2) des victimes de « spams » reposant sur des escroqueries à la loterie, i.e. abusées avec des courriers appâts qui font miroiter de grosses sommes futures mais dont la venue nécessite des frais initiaux et donc un transfert de fonds ; 3) des victimes de « romance scams », arnaques via Internet reposant sur des escroqueries à l'amour et au chantage affectif. Toutes ces escroqueries empruntent au départ le format de la « dyade électronique » : parfois dès l'origine par mail, parfois depuis une connexion depuis un site de rencontre.

Le but de l'étude, qui ne repose pas sur une analyse interactionnelle fine des dynamiques de manipulation, est de fournir un cadrage préalable sur les modalités spécifiques de la « manipulation à distance » lorsqu'elle emprunte la voie de la communication électronique. C'est ainsi par rapport à l'adhésion à la secte (Esquerré, 2009), et par rapport à d'autres modalités du « régime d'emprise » (Châteauraynaud, 2004) que cette relation peut être étudiée. Toutes ces victimes ont fait l'objet d'entretiens rétrospectifs et ont également été choisies comme ayant « surmonté » leur escroquerie, la plupart d'entre elles

4. Il s'agit de l'AVEN, association des victimes de l'escroquerie à la nigériane, fondée en 2006 et qui regroupe plusieurs centaines de membres.

(9 sur 12) se caractérisant même par le fait que, sans forcément faire partie de l'association précédemment décrite, elles sont devenues actives dans des collectifs d'aide aux nouvelles victimes et de lutte contre les escrocs. Ces communautés, sous divers intitulés[5], retournent contre les escrocs certaines des techniques de manipulation mentale qu'ils utilisent, pour récolter un maximum d'informations sur leurs méthodes de fonctionnement.

L'ordonnancement séquentiel de l'activité qui débouche sur l'escroquerie repose sur deux grandes phases chronologiques. Tout commence avec la phase de production d'un énoncé écrit, le « spam » qui va ferrer au moins une victime : la confection d'un message écrit destiné à répondre simultanément à trois contraintes pragmatiques : endormir la vigilance des logiciels anti-spam ; éveiller, par un caractère surprenant, l'attention de la victime ; abaisser la vigilance épistémique (Origgi, 2007 ; Hardvig, 1991) de la victime. La probabilité de triompher de ces trois contraintes pragmatiques est évaluée par la performance du message, calculée au vu de son taux de retour, i.e. de la proportion de « réponses » retournées par des victimes dès lors hameçonnées au spam de départ. En répondant (et le plus souvent de manière personnalisée, avec ses mots et en signant), la victime donne à l'envoyeur une information précieuse : son adresse mail est active et correspond à un humain crédule. Après cette « amorce », vient la seconde phase, au cœur de la manipulation mentale : *l'interaction à distance.* Pendant cette phase, qui va de 15 jours à 6 mois, la victime est amenée à changer de canal initial, pour aller vers des interactions plus longues et plus suivies ; le passage par la discussion par téléphone est systématique. Elle ouvre à un régime d'emprise.

Nous nous centrerons sur deux questions principales : quels sont les facteurs prévalents pour expliquer l'efficacité de la manipulation à distance dans le cas de l'escroquerie par Internet (par opposition aux autres formes de manipulation à distance) ? Par quelle modalité émerge, pour contrarier la dynamique d'engagement dans le déni et l'autopersuasion qui caractérise le « ferrage », un « trouble » pragmatique (Cefaï 2002), un éveil critique, une perplexité ? Cet éveil présuppose-t-il l'introduction de tiers, ou s'effectue-t-il de manière autodidacte ? Nous répondrons à ces questions en tentant, à partir de nos différents entretiens, de ne prendre en compte que les traits les plus communs aux différentes expériences des victimes.

---

5. Les communautés auxquelles appartiennent ces victimes « seniors » que nous avons interviewées sont http://419eater.com, http://thescambaiter.com et http://www.croque-escrocs.com/.

L'AMORCE DE LA MANIPULATION À DISTANCE : LA PRODUCTION D'UN MESSAGE « ACCROCHEUR »

Le spam est, selon la définition de la CNIL, l'envoi massif, et parfois répété, de courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière. Selon certaines sources, 80 % des mails envoyés à des particuliers seraient des spams, et 95 % chez les professionnels[6]. Selon le rapport mensuel fourni par Symantec, ce chiffre atteindrait 90,7 % des courriels émis en mars 2010, un pourcentage qui s'est nettement accru ces dernières années (il était de 80 % en 2005)[7]. À l'inverse, le scam, escroquerie abusant de la crédulité des victimes en utilisant les messageries électroniques en leur soutirant de l'argent, est, à cause du chiffre « noir » de la criminalité informatique (Lointier, 2008), plus difficile à appréhender statistiquement ; il représenterait peu par rapport à l'ensemble du courrier sur Internet, mais une part plus importante des profils sur les sites de rencontre amoureuse. D'après le FBI, il y aurait autour de 60 000 personnes émettrices au quotidien, arrosant une très grande quantité de cibles, dont un nombre réduit se ferait escroquer ; mais les sommes extorquées d'après les affaires jugées en 2010 représentent une moyenne de 20 000 dollars par victime[8].

Aujourd'hui, les deux variantes de l'escroquerie par Internet, le spam comme le scam, sont très organisés à l'échelle internationale. Concernant le spam, il est difficile pour un simple amateur isolé d'en produire avec succès ; d'une part parce qu'un simple amateur ne va pas connaître et maîtriser les bons serveurs proxy pour son envoi, d'autre part parce qu'il ne va pas avoir les techniques à jour pour tromper les filtres anti-spam qui renouvellent très rapidement leurs méthodes (Posluns, 2004, 8). Le spam est ainsi l'objet d'une division du travail très stricte, dont on peut distinguer quatre acteurs principaux : le *hacker* qui vole une base de données commerciales, ou qui la rachète à un autre pirate ; le *promoteur du spam* qui s'occupe de rédiger le message pour qu'il passe outre les filtres divers susceptibles de barrer son acheminement ; le *coordinateur* du groupe qui est responsable de récupérer et de redistribuer les profits générés ; et enfin l'*annonceur* qui veut vendre un produit en passant par ces méthodes de prospection commerciale illégales. Bien qu'il y ait une division du travail

6. Rapport annuel de la société Sophos (2009).
7. Source : Symantec mai 2009.
8. Fraude nigériane : 20 000 $ de gain par victime en moyenne [archive], SecurityVibes *(consulté le 7 septembre 2010)*.

technique marquée, les équipes sont toutes petites (il n'est pas rare qu'il n'y ait que quatre personnes). Dans tout projet de spam, le *hacker* joue un rôle pivot. Il s'occupe de pirater les bases de données commerciales, et préférentiellement vise des cibles adaptées au type de message ; par exemple, pour un spam sur le Viagra, on recherchera plutôt des *hackers* sachant pirater des bases de données de gens inscrits sur des sites pornographiques. Le second rôle, celui du *promoteur,* consiste à rédiger les messages pour qu'ils franchissent les barrages de différents filtres, tout en restant lisibles par les millions de destinataires finals. Il consiste à repérer et à utiliser des « serveurs proxy », qui sont des serveurs mandataires ayant pour fonction de relayer des requêtes entre un poste client et un serveur. Mais cela va plus loin, en termes de niveau de précision. Le « proxy serveur » (serveur mandataire) qui doit être choisi par le promoteur doit être capable de passer à travers la liste noire d'émetteurs de courrier électronique qui est généré par la plupart des DNS. Cette liste noire est le fruit d'un effort coopératif des fournisseurs de noms de domaine pour interdire le service DNS aux spammeurs connus. Les spammeurs connus sont ainsi bloqués lorsqu'ils tentent d'obtenir l'adresse IP d'un fournisseur de courrier électronique, ce qui les empêche d'envoyer leurs missives. En effet, pour envoyer un courrier électronique à un utilisateur, on doit préalablement demander l'adresse IP de son domaine, et c'est cette demande qui est bloquée grâce au service coopératif de liste noire. Le troisième rôle, celui de *coordinateur*, consiste à collecter et à répartir l'argent venu de l'annonceur. En général, l'annonceur propose une rémunération sous la forme d'un pourcentage sur les ventes générées par la campagne de prospection commerciale. Dans la plupart des cas de spams, ce pourcentage est aux alentours de 40 % : par exemple, pour un annonceur vendant du contenu pornographique, adultsupercash.com, cité en exemple dans un travail (Posluns, 2004), le tarif est de 40 % de reversement pour chaque abonnement à l'essai, ce à quoi s'ajoutent 50 % des revenus pour chaque abonnement définitif. Cet argent est ensuite reversé entre les différents protagonistes de la chaîne : le *hacker* des bases de données en reçoit une partie, le promoteur une autre.

Le scam, que certaines catégorisations de référence identifient comme un sous-ensemble du spam[9], fait aussi l'objet d'une organisation. Dans le cas des escroqueries en langue francophone, principalement venues du Bénin et de la Côte d'Ivoire, d'après la présidente de l'association AVEN, celle-ci se

9. Ainsi le fait la typologie utilisée dans le rapport mensuel sur le spam émis par Symantec.

constitue sur une base territoriale : « *Abidjan est faite de quartiers. Dans chaque quartier, il y a ce qu'ils appellent eux un lieutenant, c'est lui qui dirige le quartier, ce lieutenant est chargé de former les plus jeunes (12-13 ans ça commence) qui eux sont sur les ordinateurs dans les cybercafés à appâter les gens, à envoyer des faux mails fausses loteries, cyber-héritages tout ce que vous voulez Après, au-dessus d'eux il y a ce qu'ils appellent eux les vieux pères. C'est des gens qui vont commencer l'escroquerie et s'ils sentent que la victime est encore prête à continuer, là ça passe aux lieutenants. S'ils sentent que la victime a de l'argent, ce ne sont plus les vieux pères qui s'en occupent, mais les lieutenants* » (P., victime de scam). Les protagonistes se divisent le travail sans se connaître mutuellement. Pour cela, ils se transmettent des informations précieuses selon un code mal connu du grand public, ce qui diminue sa corruptibilité. Par exemple, une des manières pour eux de collecter des adresses, en plus de l'extraction automatiques de celles-ci sur des forums, faite en utilisant des logiciels, consiste à aller chercher les adresses qui se trouvent sur des « livres d'or », c'est-à-dire sur les sections de gratification qui existent sur des sites Web. Elles constituent de véritables bases de données d'adresses naturellement disponibles sur le Web. Or il faut encore s'assurer, lorsqu'on trouve une collection d'adresses sur un livre d'or, que celles-ci n'ont pas déjà été utilisées par un escroc. Pour cela, une coutume couramment pratiquée, entre les escrocs, consiste à renseigner sur le lieu de la collecte lui-même (en l'occurrence le livre d'or) l'information que la récolte a déjà été effectuée. L'escroc, depuis une adresse généralement forgée, affiche ainsi un code mentionnant le fait de s'être servi et donc d'avoir asséché le terrain, en utilisant un mot clef compris des seuls initiés : « mugu »[10]. Cela permet de constituer de véritables bases de données d'adresses déposées dans des sites Web.

« Faites la recherche suivante sur Google : 'Livre d'or + mugu'. Dans les pages affichées par Google, vous verrez des phrases de type : *"MUGU DEY HERE, KEEP IT UP"* ou "*Mugu Mugu Mugu* I am here" ou encore *"MUGU KEEP OFF HERE BEFORE YOU GET LOST IN"*. Ces mentions indiquent aux autres escrocs que toutes les adresses mails sont déjà la propriété d'un autre escroc, un mugu » (A., victime de scam).

10. « Mugu » est à l'origine un terme de l'argot ivoirien qui signifie « abruti ». Dans le contexte de ces attaques, sa signification s'inverse et il désigne l'escroc lui-même.

Le « spam » comme le « scam » – envoi massif de courriels non sollicités à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière – constituent ainsi une insécurité qui s'appuie sur une division du travail liée à une spécialisation fonctionnelle et respecte des règles de secret et de confinement des protagonistes de ces escroqueries, qui ne connaissent l'identité que des maillons proches d'eux dans le réseau clandestin, sur un modèle pyramidal proche de l'organisation mafieuse.

Entre exploitation des schèmes routiniers et excitation pour le nouveau : le spam comme mixte pragmatique

Les spams comme les scams, pour toucher leur cible, exploitent une double vulnérabilité de la chaîne de vigilance socio-technique. D'une part, en contrefaisant des messages normaux ou justifiables d'une attention[11] « légitime » et en s'inscrivant dans les schèmes routiniers de l'utilisateur, ils exploitent la baisse de vigilance associée à l'activité familière, ordinaire ou machinale. D'autre part, en s'appuyant sur la capacité des technologies de l'information à satisfaire la curiosité exploratoire et en formulant des promesses exceptionnelles, ils excitent l'attention voire exploitent une incapacité à réfréner cette excitation. Une première dimension consiste à comprendre comment est pris en compte et se résout cet arbitrage aux divers maillons de la chaîne de construction du spam, depuis la confection préalable de l'envoi de masse jusqu'au harcèlement individuel de la victime pour induire chez celle-ci un passage à l'acte d'achat.

Au niveau de la reconnaissance de forme, le spam est construit de telle sorte qu'il se constitue aux limites de la capacité de reconstituer la forme du mot, car le mot doit être déformé pour tromper les logiciels automatiques de filtre. Il y a ainsi un compromis entre furtivité et lisibilité. Pour éviter l'usage de mots qui seraient immédiatement détectés et renvoyés sur une liste noire, le corps du mail doit contenir des mots contenant des séquences aléatoires et ainsi écrire « V@lium » au lieu de « valium », « X@n'ax » au lieu de Xannax. Même la phrase « If you would like to unsubscribe" est parfois remplacée par "G-ive u.p", pour tromper les filtres.

11. Sur l'attention, cf. Kessous, Mellet et Zouinar (2010).

La stratégie des spammeurs consiste ainsi à déjouer la robustesse des filtres [12], tout en conservant leur potentiel excitant (lié à la présence de certains mots) pour les humains qui les reçoivent. Pour cela, ils développent des techniques d'empoisonnement pour tromper les filtres. Ces techniques consistent à placer dans le courrier une grande quantité de texte anodin (provenant de site d'actualités ou de la littérature par exemple), pour noyer le texte indésirable et tromper le filtre. Ils combattent le filtrage statistique en insérant de grandes quantités de texte anodin ou de « salade textuelle », c'est-à-dire des séquences aléatoires de mots qui semblent cohérentes mais qui ne veulent rien dire. Une autre technique pour essayer de tromper le filtre bayésien est de remplacer le texte par des images. L'ensemble du texte, ou une partie de celui-ci, est remplacé par une image où ce même texte est « dessiné ». Le filtre de pourriel est d'ordinaire incapable d'analyser cette image qui contient les mots suspects.

Mixte pragmatique, le « spam » essaie à la fois d'être anodin pour le filtre et de toucher les émotions du récepteur humain. Pour cela, il s'appuie sur des règles statistiques issues de la psychologique expérimentale. Il pratique des déformations sur les messages. Ainsi, un message-type de spam s'écrira dans l'en-tête « subject » de la façon suivante : « dru.gs. to y.o.u.r doo r ceahp. Robotic ». Ces déformations s'appuient sur le principe que les hommes peuvent aisément reconnaître des mots brouillés aussi longtemps qu'on n'en modifie pas les premières lettres. Les spammeurs utilisent ainsi des logiciels qui créent du bruit aléatoire – points ou espaces entre les lettres. Des chercheurs ont d'ailleurs mis en évidence ce résultat étonnant : qu'il y avait plusieurs milliards de façons de faire des fautes d'orthographe en écrivant Viagra, plusieurs quintillions de façons de mal écrire Viagra qui sont pourtant toutes compréhensibles par l'utilisateur de mail moyen [13].

---

12. La plupart des filtres sont fondés sur des mécanismes plus subtils que la simple mise sous quarantaine en fonction de la présence d'un mot ou d'un motif suspect. lls calculent la probabilité globale qu'un message soit indésirable en combinant les probabilités conditionnelles, i.e. les probabilités qu'il le soit en fonction de la présence de chacun de ses mots. Si le courriel contient un mot à forte « spamicité » – tel que « sexy » ou « loterie » –, les filtres ne le mettent pas immédiatement en quarantaine, mais prennent en compte aussi d'autres mots importants, comme par exemple le nom de la personne ou les noms d'amis, qui sont habituellement des signes de courriers légitimes et prendront alors le pas.

13. Cockeyed.com, "There are 600,426,974,379,824,381,952 ways to spell Viagra", 2004 (4 avril). Voir http://cockeyed.com/lessons/viagra/viagra.html.

La production de la crédulité : l'appui sur une excitation

La capacité de recueillir l'attention du récepteur n'est pas suffisante pour générer sa crédulité. L'information communiquée par un manipulateur, aussi habile soit-il, n'a une chance d'être accueillie dans l'esprit de sa cible que dans la mesure où elle y rencontre un certain écho. Lorsqu'il y a consonance avec les désirs du récepteur, l'intensité de la vérification faite par ce dernier diminue. S'il l'accueille facilement, c'est parce qu'elle « l'arrange ». Il a très envie d'y croire. Comment est-il possible de manipuler ses propres états mentaux de manière à susciter auprès de soi-même la croyance qu'une proposition désirable est vraie ? Ceci revient à se duper soi-même (Engel 1991). L'autopersuasion se réalise en couplant deux opérations apparemment contraires, l'une renvoyant à l'image idéalisée de soi et l'autre à une frustration et à un espoir de changement. D'une part, le message escroc performant fait un appel discret à des valeurs fortement partagées à l'intérieur de la communauté, comme la générosité ou la sollicitude (dans le cas d'un message appelant à collaborer à un transfert d'argent, la promesse d'argent était accompagnée de formulations explicites visant à « appeler à l'aide »), le « courage » (dans le cas d'une romance par Internet). D'autre part, le message renvoie à des excitations s'appuyant sur un fond de déception : dans les cas étudiés ici, cela renvoie à l'éveil de la cupidité (participer à une loterie ou au partage d'un « trésor »), à la promesse d'une meilleure santé, à l'excitation d'une relation amoureuse souvent exotique.

Une particularité majeure du régime d'emprise est qu'il vise, tout en installant une habituation destinée à tromper la vigilance de la victime, à déployer de nouvelles péripéties toujours étonnantes configurées sous la modalité d'obstacles contrariant la bonne réalisation de la transaction et ayant un caractère dilatoire. Cet enchaînement de péripéties repose assez largement, à ce stade, sur la multiplication des actants voire des interlocuteurs – l'interaction avec la victime étant le plus souvent progressivement distribuée entre une variété d'émetteurs se présentant comme distincts : le témoin initial, un avocat, un banquier, etc. Cela amène la victime à tournoyer entre plusieurs interlocuteurs, ce qui peut provoquer un sentiment de vertige : les victimes mentionnent l'idée d'être prises dans un manège arrivant, selon les termes de l'une d'entre elles, à leur « *donner le tournis* ».

LA MANIPULATION À DISTANCE ET LA SPÉCIFICITÉ DU RÉGIME D'EMPRISE PRODUIT PAR INTERNET

La relation d'« emprise » démarrant à partir du moment de l'hameçonnage, se décompose en deux phases. Une première phase organise l'échange de mails autour de la multiplication de péripéties sur le canal de départ. Ensuite, il advient nécessairement une phase où l'interaction bascule sur un autre canal, et notoirement se transporte vers un medium qui supporte l'échange synchrone et faisant transparaître la voix ou le visage. Dans la quasi-totalité des cas, il s'agit du téléphone : la victime est enjointe de donner un numéro, et se fait appeler de manière brève, mais régulière, pour qu'elle rappelle à son tour ses interlocuteurs. Cette seconde phase peut être dite de *harcèlement téléphonique.* Elle amène à l'orée du processus, recherchée depuis le départ par le malveillant : l'extorsion proprement dite, où l'argent de la victime est recueilli. Lors de l'extorsion s'opère quasi systématiquement un mécanisme de surenchère par lequel lorsqu'une première livraison se réalise – soit de documents officiels attestant d'une identité, soit d'argent via un organisme de transfert international de fonds, un mécanisme de retardement ou de dilatation de la résolution intervient, par lequel l'escroc effectue alors une demande supplémentaire, justifiée par l'énoncé d'une péripétie malheureuse, ce qui génère alors souvent une seconde livraison, et crée parfois un cycle d'amplifications itérées des demandes et des dons.

La production de la désorientation et du vertige

Toute relation d'emprise peut être caractérisée comme fondée sur une asymétrie de prise (Châteauraynaud, 2001) : le terme, dans une perspective interactionniste, peut décrire une dissimulation d'une frange du cadre de son expérience à une autre personne, constituant ce que Goffman (1990) décrit comme une fabrication. Mais la notion d'emprise engage un trouble dont la description suppose la mobilisation d'une littérature plus attentive aux attributs émotionnels de cette situation, au premier titre desquels on trouve la perte d'orientation induite par les situations où s'affrontent des forces non calibrées, incertaines, comme c'est le cas dans les dynamiques de sorcellerie ou d'ensorcellement (Favret-Saada, 2001).

Un trait général de la relation d'emprise est ainsi d'avoir pour caractéristique la difficulté de garder l'autonomie individuelle ou un horizon de réflexion et de calcul.

L'exemple de la manipulation exercée sur un médecin piégé par un tarif élevé auquel il a souscrit par Internet illustre la modalité la plus fréquente par laquelle s'exerce l'emprise : la tromperie sur l'attention, la fabrication d'une illusion représentationnelle.

> Monsieur M., médecin à Paris, reçoit un spam sur sa messagerie électronique ayant toute l'apparence d'un message à caractère professionnel. En effet, il évoque une pathologie bien connue – le diabète – et propose au médecin de recevoir un document faisant le point sur les dernières recherches en matière de diabète de type 1 (insulino-dépendant) et de diabète de type 2 (non insulino-dépendant) ainsi que sur les derniers traitements permettant la prise en charge des patients.
>
> Pour recevoir cette documentation, le médecin doit remplir un certain nombre de champs lui demandant son état civil ainsi que certains renseignements professionnels et cocher quelques cases signifiant son accord sur divers points.
>
> Étant intéressé par cette pathologie et souhaitant être au fait des dernières avancées de la médecine en la matière, Monsieur M. remplit rapidement le formulaire et le renvoie.
>
> Ce à quoi Monsieur M. n'a pas fait attention, c'est que le message électronique comprend en bas de page un petit codicille précisant que le renvoi du formulaire complété équivaut à une inscription du médecin sur un annuaire international sur Internet et suppose le paiement d'une redevance d'environ 1000 euros.
>
> Compte tenu du nombre de messages électroniques et de courriers papier que reçoit ce médecin tous les jours, il lui est rigoureusement impossible d'accorder un temps important à chacune de ses correspondances et le petit paragraphe de bas de page lui a évidemment échappé.

Cette arnaque connue provient d'une société suisse dénommée NovaChannel spécialisée dans l'édition en ligne de guides internationaux à destination de touristes. Le but et le procédé sont toujours les mêmes : il s'agit de répertorier des commerçants ou des professions libérales dans un annuaire en ligne et de leur faire payer ce service de publication. Pour l'heure, de nombreux professionnels dont des médecins français et étrangers se sont faits abuser. Cependant, compte tenu de la législation en vigueur dans les différents pays européens, il est en général conseillé de ne pas les payer car leurs actions en justice seraient nulles et non avenues. Le principe de l'arnaque est donc relativement simple et semble bien fonctionner puisqu'au vu des forums, de nombreux médecins et thérapeutes se sont faits abuser de cette manière. Il semble même que, parmi

ces professionnels de santé, ils sont nombreux à s'être acquittés de leur dette de peur d'être poursuivis judiciairement. À la différence des spams classiques qui sont envoyés à des millions d'exemplaires, ce type de spam est très ciblé et la rédaction est élaborée en conséquence.

La provocation de l'excitation curieuse fonctionne ici sur le modèle d'une tromperie portant sur la vigilance du médecin généraliste. De ce point de vue, le spam est construit pour être adapté aux failles de vigilance du médecin généraliste, et donc sur une anticipation de son mode de travail. Ce dernier fait en général face à un emploi du temps très serré constellé de nombreuses tâches : réception des patients, coup de téléphone de patients, échanges avec les confrères (médecins spécialistes, médecins hospitaliers, laboratoires d'analyse…), tâches administratives, lecture et réponses aux mails et aux courriers papier… Tous les médecins expliquent que l'accomplissement des tâches administratives et les réponses aux diverses sollicitations supposent assez systématiquement de remplir des questionnaires leur demandant leur lieu d'exercice, leur spécialité, leurs horaires, les pathologies soignées… Ce type d'activité étant tellement fréquent, il est quasi systématique que les médecins ne lisent pas l'ensemble de la documentation envoyée. La stratégie de l'escroc est clairement basée sur ce point : le médecin va remplir le questionnaire quasi automatiquement sans se préoccuper des paragraphes d'explications se situant souvent à la fin des documents en ligne ou sur papier. Dans ce cas, c'est clairement ce qui s'est passé : le médecin a renseigné l'ensemble des champs présentés, ne lit pas le petit codicille qui l'engage (codicille écrit en caractères plus petits que le reste du contenu) et transmet le document.

Lorsque nous avons interrogé pour la première fois ce médecin, il nous avait relaté sa déconvenue mais ne semblait pas encore certain de l'enchaînement des événements ; en tout cas, il n'arrivait pas à comprendre de quelle manière il avait pu être victime de cette escroquerie. Son interrogation première concernait les raisons qui avaient pu le pousser à adhérer à un annuaire international de médecin. En effet, et sans trahir ses propos, il nous a expliqué qu'il avait plus de soixante ans, qu'il était médecin généraliste depuis plus de trente-cinq ans et que tant sa pratique que sa structure psychologique ne pouvaient le pousser à souhaiter de la visibilité professionnelle. Par conséquent, il estimait de bonne foi qu'il était impossible qu'il ait pu être sensible à une inscription sur un annuaire international de médecins. Par ailleurs, étant un médecin de quartier heureux, il n'avait que faire d'être référencé *urbi et orbi*. Le « spam » a réussi car il a surtout trompé la capacité de discernement de l'individu en se coulant dans une familiarité.

À la suite du renvoi de ce formulaire rempli censé lui permettre de recevoir une information professionnelle sur le diabète, Monsieur M. reçoit un courrier papier lui demandant de renseigner un questionnaire plus détaillé sur son lieu d'exercice, ses spécialités. Là encore, un codicille bien masqué évoque le sujet de la liste des médecins internationaux ainsi que la redevance afférente et là encore, Monsieur M. n'y prête pas vraiment attention. La suite de l'arnaque est relativement simple. Monsieur M. reçoit ensuite une lettre lui expliquant qu'il allait avoir l'honneur d'apparaître sur une liste internationale de médecins sur le site Med Web [14] spécialisé dans les « informations médicales internationales et bases de données ». Cette lettre précise également que cette publication suppose le paiement d'une somme forfaitaire (environ 1000 euros) à payer par retour de courrier. Monsieur M. est au départ interloqué puis comprend ensuite l'arnaque : à l'aide d'un appât – de l'information professionnelle –, les médecins se trouvent engagés dans un accord qu'ils n'ont pas vraiment vu venir. En l'espèce, ce médecin a refusé de payer et reçoit régulièrement des mises en demeure de paiement de ce qu'il est censé devoir. La note a été réévaluée au fur et à mesure pour atteindre la somme de 4000 euros. Monsieur M. est régulièrement relancé par courrier voire lettre recommandée et a même reçu un appel téléphonique d'une prétendue avocate ayant pour mission de trouver un accord amiable à cette affaire. Signalons tout de même que le nom de Monsieur M. apparaît bien sur le site évoqué plus haut avec la bonne adresse d'exercice ! Si le médecin paye ce qu'il est censé devoir, le rapport de force se conclut favorablement pour l'escroc ; en revanche, si le médecin refuse de payer, on entre dans une étape caractérisée par « un déchaînement de forces » [15] qui peut supposer l'engagement de territoires et de machines. En effet, le combat qui va se dérouler va mettre aux prises les deux protagonistes avec des moyens légaux – lettres de relance par l'escroc, saisie d'un avocat et de la Direction générale de la consommation, de la concurrence et de la répression des fraudes par le médecin – et des moyens plus répréhensibles – coup de téléphone d'une présumée avocate de la société Nova Channel au domicile du médecin pour exercer une pression. À ce stade, le rapport de forces s'équilibre en apparence car la société Nova Channel n'obtient pas gain de cause. Dans les faits, même si le médecin ne paye pas, il est psychologiquement atteint par ce harcèlement qui met en jeu son système de valeurs. En effet, le médecin est un légaliste et le système de codification installé par l'escroc se base entièrement là-dessus : il y a un contrat et il faut

14. http://www.med1web.com
15. Au sens de Châteauraynaud.

le respecter. Par conséquent, pour lutter contre l'escroc, le médecin doit finalement lutter contre son propre système de valeurs, ou plus exactement contre le subterfuge que lui impose l'escroc quant à son système de valeurs.

C'est cependant de toute relation à forte connotation émotionnelle ou affective que l'on peut dire qu'elle est marquée par l'asymétrie de prise. Il est en effet difficile aux personnes – en relation de passion – de faire le départage entre une relation de manipulation, marquée par l'instrumentalisation contrôlée par un des protagonistes, et une relation simplement marquée par la passion mutuelle, qui se caractérise par la difficulté de s'appuyer sur des repères conventionnels ou des équivalences (Hennion, 2001). Dans le domaine amoureux, exemple extrême, celui qui aime ne calcule pas, et précisément au moment où il se met à « calculer », à se prendre ses distances ou à comparer la relation, il est conduit à quitter l'état d'emprise amoureuse (Boltanski, 1998)[16]. Dès lors, la relation de manipulation est d'autant plus difficile à détecter qu'elle s'inscrit dans le domaine passionnel, où les repérages sont plus difficiles à identifier. Cette difficulté à discriminer est une source supplémentaire de désorientation.

La spécificité d'Internet : la production d'un isolement complet pour la victime

Pour qu'on puisse attribuer à une relation la qualification de « manipulation mentale », il faut que la recherche de pouvoir ou de « prise » sur un individu s'exerce avec la tentative de le faire rompre avec son environnement d'origine : par opposition au simple embrigadement, la manipulation mentale s'appuie sur la recherche de déstabilisation mentale et d'isolement de la victime par rapport à son entourage proche.

16. En effet, c'est de toute relation amoureuse naissante que l'on peut dire qu'elle est piégée au sens où la rencontre amoureuse est par définition fondée non sur un consentement, mais sur des asymétries de prise (Châteauraynaud, 2007) ou sur ce que Lacan appelle une « méprise ». Comme l'indique, après bien d'autres, le célèbre psychanalyste, « aimer c'est donner quelque chose qu'on n'a pas à quelqu'un qui n'en veut pas ». Dans la rencontre, il y aurait ainsi deux dispositions qui se rencontrent, chacune avec ses propres séries de projections et d'attentes. Ce qui circule des la relation amoureuse naissante est dès lors de l'ordre d'une absence de compréhension commune : quand j'aime, par exemple, il se peut que j'aime surtout parce que je surinvestis un acte qui me permet de combler une frustration qui m'était préalable ; il se peut tout aussi bien que j'aime narcissiquement, à travers le regard aimant de l'autre, une image de moi-même qui m'est alors renvoyée. Ce qui caractérise la relation amoureuse est le déséquilibre dû à des surinvestissements imaginaires de l'autre.

Cependant, la manipulation mentale, lorsqu'elle s'opère dans des cadres de coprésence, comme lors de l'adhésion et de l'évolution d'un individu dans une secte, s'établit rarement dans l'ignorance de l'entourage. Elle a un coût social dans la mesure précisément où l'entourage l'apprend, fortuitement ou par le fait que la victime le dit publiquement. Ainsi, l'entrée dans une secte entraîne souvent une rupture des liens sociaux. Cette rupture est essentiellement due à une réaction de rejet, aussi bien par les proches, la famille ou les amis, que par les personnes avec lesquelles l'adepte entretient des relations professionnelles. Le rejet des membres des sectes a même suscité un sentiment de honte chez les proches des adeptes, et notamment les familles. C'est d'ailleurs cette honte qui fut à l'origine de la mobilisation des associations de défense des victimes, dans les années 1980, qui a été à l'origine initiée par les proches des adeptes et non par les adeptes eux-mêmes. Comme le note Esquerré (2009, p. 138), « les proches des adeptes ont entrepris de ne plus vivre ce qui leur arrivait en cachette, mais de lui donner au contraire la plus grande visibilité possible, en attirant l'attention des pouvoirs publics et des médias et en affichant une certaine fierté d'affronter le danger sectaire ». La rupture des attachements consécutive à l'entrée dans la secte est le produit d'une communication auprès des proches.

C'est ainsi une caractéristique distinctive de la relation de manipulation mentale par Internet que de renforcer l'isolement de la victime. Newman et Clarke (2003) ont insisté sur cette caractéristique dans les escroqueries sur Internet. L'isolement de la victime par rapport à son réseau relationnel est rendu possible par le fait que la relation s'effectue dan un contexte marqué par une discrétion nouvelle, alors que dans la manipulation mentale classique la relation est difficilement dissimulable.

L'engluement dans l'autopersuasion est souvent rapporté par les victimes à l'isolement dans lequel elles ont été confinées.

> L'escroc essaie toujours d'isoler sa victime : il lui dit de n'en parler à personne. Donc, comment en parler, puisqu'on n'a pas dit le début et on n'a rien annoncé. Moi j'ai une dame qui s'est fait escroquer de 80 000 euros (c'est encore petit comme montant), c'était l'héritage de son mari elle était veuve depuis deux ans, c'était destiné à son fils unique, comment voulez-vous qu'elle lui dise ça ? (id.).

L'isolement est particulièrement clair dans la phase 3, celle du harcèlement téléphonique. Lorsqu'il appelle (il préfère systématiquement se faire appeler)

l'escroc va communiquer avec la victime de manière très brève, en lui disant toujours de le rappeler à un moment où elle sera seule.

> Donc, comme on n'en a pas parlé autour de nous, on va devoir s'isoler pour lui parler. Dans toutes ces escroqueries, on vous dit toujours : n'en parle à personne, c'est très confidentiel (M., victime de spam).

Si la victime dit qu'elle en a parlé à quelqu'un d'autre, elle se fait réprimander. L'escroc va alors chercher à rentrer en contact avec la personne mise au courant pour éventuellement la manipuler à son tour.

> Puisqu'elle n'a pas alerté la première victime à qui elle l'a dit ça veut dire que l'autre n'est pas au courant de ce qui se passe et qu'éventuellement… (B., victime de spam)

La pratique, dans les associations de lutte contre les arnaques, de défis où il s'agit d'extraire et collecter le plus possible d'informations sur les producteurs de spam peut nourrir enfin une imagination du complot.

> Dans ses CGU, Western Union a mis : n'envoyez pas d'argent à quelqu'un que vous ne connaissez pas ; moi je dis stop (…). Quand on envoie de l'argent à Western Union, il y a toujours une petite case à cocher, quand on la coche, qui dit que le destinataire aura une pièce d'identité en cours de validité. Quand on fait une réclamation à la Poste puisque c'est le représentant de W.U. en France, ils sont incapables de dire quelle est l'identité qui a reçu les fonds, est-ce qu'il y a un numéro de pièce d'identité etc. Pourquoi ? Parce que les agents de W.U. sur place font partie des réseaux. Alors bien sûr la victime, la première chose qu'elle cherche à faire, c'est de récupérer son argent, mais il n'y a pas moyen. Il n'y a aucun moyen. Pour la poste, l'argent a été retiré par la personne à qui le mandat a été fait. Point. (B., victime de spam).

Par conséquent, la contestation reste muette, vécue sur le mode d'une douleur personnelle dont il est difficile de témoigner. Le chiffre noir du spam est important. Ainsi, l'agressivité des spammeurs est d'autant plus marquée qu'ils affrontent des consommateurs confinés dans un ordre intime, et réticents par rapport aux formes publiques, ou prisonniers de l'inavouable. Des systèmes de dénonciation anonyme (comme Signal Spam) contribuent à prendre en charge ce problème.

> Les gens ne portent pas plainte pour toutes sortes de raison, comme la honte, la culpabilité. Il peut y avoir la culpabilité d'avoir vendu les biens familiaux – il

> y en a qui vont très loin, qui vendent les maisons, qui balancent les héritages. Je dirai que c'est maintenant 80 % des plaignants qui se voient refuser une plainte. Certaines fois, on leur dit : vous êtes bien naïf. Dans l'association, je pense qu'on représente 10 % des victimes, donc c'est très très peu, en France principalement (C. responsable associative).

L'association d'aide aux victimes recommande ainsi aux particuliers qui anticipent un rejet de leur plainte au commissariat, et qui ont ainsi peur des quolibets ou des moqueries souvent proférées de manière publique à l'intérieur de celui-ci, de ne pas hésiter à déposer plainte directement auprès du Procureur de la République du tribunal d'instance de son lieu de domicile.

L'isolement relationnel est ainsi le facteur principal de l'entrave mise à la plainte de la victime.

Mais d'autre part, l'éloignement, la distance difficile à franchir physiquement sans coût très élevé, mais aussi l'écart interculturel, diminue l'inhibition de l'escroc. L'éloignement permet à l'escroc de sous-estimer, de plus facilement dénier, le mal causé. Les escrocs en ligne développent trois principales techniques de neutralisation afin de rationaliser leurs activités avant d'escroquer leurs victimes. L'escroquerie peut être considérée comme une punition envers une personne qui le mérite : leur proie était « avare et complice » (Dixon, 2005). Ils ont souvent leurs propres hymnes (rengaines fredonnées ou chantées) tels que « I Go Chop Vos dollars », une chanson dont le refrain est par ailleurs accompagné de couplets comme « Vous être le Mugu [la victime], je suis le maître... Je vais couper votre dollar, je vais prendre votre argent et disparaître. L'arnaque (4-1-9) est juste un jeu, vous êtes le perdant, je suis le gagnant » (Finckenauer, 2007). Un genre musical, le « couper-décaler », est d'ailleurs constitué dans certains pays d'Afrique noire et rassemble l'ensemble de ces chansons et refrains. Une autre technique de neutralisation consiste à insister sur le fait qu'il n'a pas été causé de préjudice corporel ou de blessure aux personnes.

Les réseaux d'escrocs opérant par romance par spam développent une sous-culture, la « scam culture ». Beaucoup appartiennent à des groupements d'individus qui mettent en commun l'argent gagné, partagent les ressources informatiques, les listes d'adresses e-mails, l'accès Internet, et entraînent les nouveaux venus aux techniques et à l'art de persuader par mail, par messagerie vocale et parfois par contacts téléphoniques. Ces nouveaux venus n'ont parfois pas plus de six ans (De Brosse, 2008). Il est ainsi fréquent que les scammers gèrent un

nombre de relations simultanées de l'ordre de la dizaine (Bruillard, 2009). Sefi Atta (2009) raconte les stratégies de déni du mal causé mises en œuvre par les escrocs ; il se développe souvent un grandissement civique de l'escroquerie, selon une explication mettant en évidence le fait que les victimes appartiennent à un pays riche, ou sont cupides. De manière plus sophistiquée, il y a l'argument que l'escroquerie renvoie à la culpabilité de victimes par rapport à leur grande richesse, ce qui expliquerait qu'il n'y a pas à se culpabiliser d'envoyer ce genre de mails aux gens.

ENTRE ENGAGEMENT DANS LE DÉNI ET INQUIÉTUDE CURIEUSE : LA DYNAMIQUE D'ÉMERGENCE DU TROUBLE

Enfin, il faut remarquer que le processus d'acquisition et de mémorisation des idées contre-intuitives suppose un long cheminement qui implique de la part de celui qui désire accéder à ces idées un engagement personnel considérable. Les efforts consentis à chacune des étapes de l'initiation ont ainsi de fortes chances de rendre à ses yeux très précieuses les représentations ainsi transmises. Plus l'effort fait pour acquérir une connaissance a été important, et moins la valeur intrinsèque de ces connaissances aura de chances d'être mise en doute par ceux qui les ont péniblement acquises (Cialfini, 1984, p. 88). Ainsi, bon nombre de représentations de victimes de spam, du fait qu'elles entrent en contradiction avec les attentes intuitives, se détachent de manière particulièrement saillante par rapport à d'autres représentations. Elles ont donc tendance à s'imposer durablement à l'attention de leurs victimes. Comme le remarque Pascal Boyer (1992), les mystères qui ont le plus de chances de s'imposer sont ceux qui se rapprochent d'un optimum cognitif qui combine déclarations intuitives et contre-intuitives. Un équilibre est alors atteint entre l'appel à l'imagination et la facilité à être mémorisé. Dans tous les cas de manipulation, la victime décrit rétrospectivement son cheminement en renvoyant à l'idée d'un « cercle vicieux » ou d'une autopersuasion liée à la difficulté de remettre en cause le « premier pas » réalisé dans l'engagement, ou le prêt de croyance initial.

L'engagement comme déni : dynamique d'enfermement de la victime

Il y a ainsi un long moment, durant la relation, qui est marqué par le déni. C'est une modalité sur laquelle a insisté Berg (2009). Le moment où elles acceptent de s'avouer qu'elles ont été victimes d'une manipulation est très

coûteux émotionnellement. Non seulement elles expriment du ressentiment, de la colère, de la douleur, mais également, comme le note Berg, de l'auto-culpabilisation, une perte d'estime de soi, une diminution de confiance et une angoisse à continuer d'avoir des relations en ligne. Une des raisons du déni est le fait que, ayant fait le premier pas, en mordant initialement à l'hameçon, les victimes ont du mal à se remettre en cause. Les théories psychologiques sur le consentement volontaire et la manipulation [17] ont bien insisté sur le fait que les stratégies les plus persuasives sont celles qui incitent l'individu soumis à s'engager dans sa décision, par exemple à assumer ses choix ou à les revendiquer. L'engagement est ainsi le lien qui relie l'individu à ses actes. De plus, les individus que l'on oblige à réaliser un acte extorqué se retrouvent dans une situation de dissonance, et donc s'efforcent de réduire cette dissonance en mettant en rapport leurs idées ou leurs connaissances avec leurs actes.

Il existe en outre un *frisson* particulier chez les victimes de certains harcèlements suite à des spams, qui est lié à l'irruption d'un événement inexplicable dans une vie quotidienne banale. On pourrait parler d'une séduction pour l'étrange. Celle-ci consiste à se laisser sentimentalement charmer par ce à quoi on ne croit pas ou plus, voire à ce à quoi on est gêné de croire, dans un conflit entre les croyances et l'attitude jugée raisonnable, proche de ce que l'ethnologue Arnold Van Gennep a appelé le « oui-mais », qui consiste à affirmer ne pas croire tout en croyant quand même. La fascination ou vulnérabilité narrative – qui est à la source du plaisir d'écouter un bon récit – a toujours été renforcée par l'irruption régulière, dans la trame narrative, d'événements inattendus, ceux que le récit appelle des « péripéties ». Quelque chose va de travers, sinon il n'y a rien à raconter (Bruner, 2002). Parfois, le rythme de ces péripéties est jugé trop lent. Proust, commentant l'écriture de Flaubert, a pu exprimer un sentiment de monotonie et comparer la lecture à la circulation sur un « trottoir mécanique roulant ». Par les rebondissements et donc le suspense qu'elles génèrent, les péripéties créent une implication forte.

> Il y a même des escrocs qui envoient des fleurs ou des petits bijoux (S., victime de scam).

La péripétie peut aboutir à un prolongement inhabituel de l'échange.

> J'ai connu des gens qui continuent de discuter avec un escroc pour savoir pourquoi il a fait ça, si tu m'avais demandé normalement j'aurais pu le faire, et là

17. Parmi celles-ci, Joule et Beauvois (2006).

> on peut carrément déboucher sur des mariages gris ! L'escroc continue, une fois démasqué. Son problème, à l'escroc, c'est de quitter l'Afrique. Il va se faire épouser, celle ou celui qui épouse l'escroc ne saura pas qu'il va se faire escroquer, c'est le propre du mariage gris, et une fois que l'autre est en Europe et a obtenu ses papiers, ciao. Cela peut donc déboucher aussi là-dessus (T., victime de scam).

Le fil narratif, pour générer une telle attente, s'apparente à une promesse toujours différée ; on fait miroiter une certaine fin, heureuse, mais on multiplie les rebondissements et les contretemps, on additionne les péripéties selon une intensité croissante de leur gravité.

Il ne suffit pas que le contenu excitant soit « à une portée de clic ». Il faut paramétrer l'amorce, la rendre suffisamment alléchante, pour qu'elle génère une disposition à payer. Les sites identifiés comme les plus performants par les spammeurs sont précisément dessinés pour faire en sorte que le visiteur doit tourner et tourner dans une forêt de pop-up avant de pouvoir s'en sortir. Les pop-ups s'ouvrent et entraînent l'utilisateur dans une forêt de femmes attractives. Ce piège consistant à augmenter le coût de la sortie est une technique couronnée de succès ; en élevant le coût de résistance à la tentation, elle redresse sensiblement le taux de retour.

Le basculement vers l'excitation curieuse se réalise toujours selon une modalité majeure : pour se déciller les yeux, pour arriver à « redescendre de son petit nuage », il faut être confronté à des preuves objectives de la malveillance. Pour cela, il est nécessaire d'organiser une collecte systématique des tournures de phrase, des noms et prénoms forgés employés, des principales variantes d'escroqueries. Ainsi, pour déciller les yeux de la victime qui s'aveugle, la principale association francophone de victimes de spams a eu tendance à constituer une base de 23 600 adresses mails d'escrocs[18]. Elle confronte alors les victimes, encore dans l'illusion, avec des occurrences innombrables de phrases, photos, noms propres, identiques à ceux qui leur avaient été fournis par leur « escroc » dans le cadre d'une relation prétendument originale et singulière.

Un élément décisif de preuve est la découverte des photos utilisées par les escrocs pour berner leurs victimes. Ce sont souvent des photos qui ont été volées sur Internet. Elles sont difficiles à retrouver pour un individu solitaire.

---

18. Lisible sur http://www.croque-escrocs.fr /blackliste.

« *C'est comme retrouver une aiguille dans une boîte de foin* » (P., victime de scam). Toutefois les individus, pour se prouver à eux-mêmes qu'ils ont bien été escroqués, ont besoin de ces modalités d'identification. Une fois qu'on leur a montré que la photo d'identité est une photo volée, qu'on peut trouver ailleurs sur Internet, l'opération est réalisée sous la forme de l'obtention d'un indice manifeste et concordant.

L'émergence du trouble : l'inquiétude curieuse

Peu à peu, les victimes de ces spams, et notamment au cours de la phase d'extorsion proprement dite, voient monter leur perplexité, ce qui éveille en eux des soupçons ou des montées d'incrédulité. Cependant, sans l'apport d'une aide extérieure, il leur est difficile de bien se détacher de leur situation fascinée. Bien souvent, le détachement aboutit à un réinvestissement de l'intérêt curieux pour une meilleure identification des escrocs et par la participation individuelle, dans le cadre d'un collectif organisé, à leur traque. Les « scambaiters » (croqueurs de spammeurs), justiciers bénévoles s'amusant à contacter sous une fausse identité des spammeurs et prolonger le plus longtemps possible la relation, permettent le remplacement de la fascination curieuse par cette nouvelle excitation exploratoire.

Comme le note un responsable d'une organisation d'entraide :

> Quand quelqu'un vous appelle, c'est qu'il commence à devenir incrédule, à avoir des doutes… Bien souvent, il cherche une confirmation. Parfois, avec l'espoir qu'on lui dise : non, ça n'est pas une escroquerie. Mais la plupart du temps, c'est des gens qui cherchent une confirmation. Et là on voit d'autant plus qu'ils sont très bien manipulés parce que c'est très dur de démontrer qu'ils ont été bien escroqués (C., responsable associative).

Lorsque l'escroc se sent dévoilé, il n'y a plus de nouvelle. Aucune victime d'ailleurs ne le fait spontanément. La victime le fait pour voir si ce que nous lui avons dit est juste. Et là l'escroc disparaît.

> Moi, j'ai une personne qui s'est annoncée qui était escroquée depuis plusieurs mois, qui se doutait bien qu'elle était escroquée et qui voulait une confirmation. Je lui ai écrit par mail, je ne sais plus pourquoi, je ne pouvais pas l'appeler, ou je n'avais pas le temps, bref, elle a renvoyé mon mail à l'escroc. Qui lui a remanipulé de plus belle en lui disant : non, fais attention, cette attention, ça doit être des escrocs, ils vont te prendre ton argent, c'est comme ça qu'ils font (id.)

Le *scambaiting* existe partout dans le monde (notamment aux États-Unis, en Angleterre, Allemagne, Australie, Suède, Chine…).

> On se fait passer pour des copains à eux, on est en lien avec eux sur leur blog. Pour tout dire, j'avais commencé par Croque-escrocs. Le *scambaiting* francophone est récent, à ma connaissance je suis la première à avoir publié ma correspondance. J'ai commencé en 2004, en répondant par jeu à un scam très connu (A., victime d'une escroquerie).

C'est une activité qui est décrite comme « faisant appel à l'écriture de fiction, à l'imagination, à la création d'images, à la critique face à l'absurde de nos sociétés et à la réaffirmation de soi et de ses idées ». « J'aime bien quand mon personnage tombe amoureux de l'escroc [cf. exemple ci-dessous], ça permet de faire entrer en scène des situations encore plus loufoques et jouer dramatiquement sur les problèmes qu'apportent les passions intenses. L'idée, c'est de mener l'action comme dans un scénario de film, naturellement et lentement ». Elle est souvent considérée comme un jeu, un jeu « sérieux » (sur un modèle qui ressemble au *serious game*) et risqué :

> Un jeu de rôle mais avec des vraies personnes qui incarnent de faux personnages (B., victime de spam).

Certaines anciennes victimes pratiquent le *inver*se scam, qui consiste à arnaquer l'arnaqueur et à lui soutirer de l'argent. Cette partie comporte de nombreuses variantes : le *trash baiting*, qui consiste à conclure une vente avec un escroc et à « *lui envoyer une centaine de kilos d'ordures dans un colis pour lequel il devra payer 6000 euros de frais d'envoi dès réception* » ; ou le *vide* safari, qui consiste à donner un rendez-vous à l'escroc et à le filmer ou à le photographier à son insu. Ces pratiques procurent un frisson d'excitation aux anciennes victimes, susceptible de prolonger le régime émotionnel d'excitation qu'elles ont vécu initialement, comme le stipulent les nombreuses précautions dont sont entourées ces pratiques (notamment la proclamation qu'elles sont « *interdites aux débutants* »)

> La satisfaction, c'est d'arriver à ce que l'escroc fasse quelque chose pour nous, et d'obtenir ainsi un « trophée ». Plus le trophée est difficile à obtenir, plus il a de la valeur… On commence par récupérer un texte ou un formulaire marrant écrit de la propre main de l'escroc. Plus fort : un fichier audio avec sa voix, une chanson qu'il chante lui-même ou un texte que vous lui faites réciter (A., victime de romance scam).

Un site, 419eater.com, rassemble une incroyable collection de « trophées » où l'on peut voir des escrocs jouer de la guitare, mettre un poisson sur leur tête, tenir une pancarte avec un message absurde... Les méthodes et leurs stratégies épluchent une littérature grise de conseils émanant de spammeurs professionnels spécialisés (pornographie, loterie, tourisme). L'activité de croque-escrocs est liée à la volonté de mieux connaître les victimes.

La difficulté à produire une dénonciation publique à cause de la fascination curieuse

Au-delà de la cupidité ou de la vulnérabilité à des messages valorisants faisant miroiter des choses très favorables, il semble qu'une excitation humaine permanente soit à la racine de la vulnérabilité au spam : la fascination pour un récit curieux. De la même façon qu'on aime assister aux tours d'un bon magicien, ou qu'on aime entendre des histoires parfois à « dormir debout », certains utilisateurs se laissent volontiers entraîner dans les méandres d'une chaîne de spams à cause des péripéties narratives parfois assez fabuleuses qu'elles déroulent devant eux. Elles adoptent alors spontanément une attitude qui consiste à « suspendre l'incrédulité », un peu comme si elles se trouvaient devant le déroulé d'un récit à feuilletons. La suspension consentie de l'incrédulité décrit l'opération mentale effectuée par le spectateur d'une œuvre de fiction qui accepte, le temps de sa consultation de l'œuvre, de mettre de côté son scepticisme.

Cette fascination explique souvent la persévérance dans l'échange dans les phases d'interaction distante puis de harcèlement téléphonique lors des attaques. Une telle crédulité naturelle pour les bonnes narrations dans ces phases est liée au fait que le média Internet offre une situation où le danger se situe clairement « à distance », sans risque de contamination directe de la victime. Cela installe de fait plus naturellement une situation où il est possible d'établir une coupure stricte entre les événements vécus par ce média et la réalité de la vie de la personne. Du fait que la victime est éloignée, qu'elle communique via un nombre pauvre de canaux, que le danger, lorsqu'il est pressenti, est canalisé ou endigué dans d'étroites limites, il est possible de vivre l'expérience relationnelle comme une « réalité inventée ». La distance protège, même si réciproquement elle peut conduire à moins d'empathie. « *On est face à des sociopathes quand même. Dans les retours qu'on a par rapport aux escrocs, c'est le critère type du sociopathe : l'autre n'existe pas. Il s'en fout du mal qu'il fait, il ira jusqu'au bout. Sa victime n'existe pas, pour lui ce qu'il fait c'est normal* » (P., victime de scam).

CONCLUSION

L'article a montré comment la construction de ces chaînes de message, reposant sur une division fonctionnelle du travail, cherche à susciter la vulnérabilité crédule en s'immisçant dans des habitudes routinières tout en exploitant, pour constituer une saillance, une curiosité. Puis, l'article a cherché à identifier, lors des trois étapes qui suivent l'amorce, l'interaction distante, le harcèlement téléphonique et l'extorsion, comment s'institue une relation marquée par les rebondissements narratifs et les péripéties. À ce stade, le spam construit une relation qui installe le récepteur entre étourdissement et vertige.

En détaillant les modalités de la construction de la « manipulation à distance » à partir de l'opposition entre la production d'un *écrit* préalable (construit pour ferrer un maximum de jobards) et l'entretien ultérieur d'une interaction visant à entraîner la victime dans un régime d'emprise, marqué par la désorientation et le vertige, nous avons cherché à mettre en évidence une spécificité centrale d'Internet à la relation. L'isolement relationnel de la victime renforce la difficulté à prendre conscience de la manipulation. Les opérateurs d'une « sortie » hors de ce régime de crédulité ou d'emprise exigent l'appui sur des indices extérieurs : à quelles conditions les victimes « ouvrent-elles les yeux » ? Comment se produit l'arrêt de la dynamique d'enfermement crédule, qui s'appuie sur l'habituation et l'engagement progressif de la victime dans le déni et l'autoconviction ? Quels sont les opérateurs de passage pour que s'institue, à l'inverse, une dynamique d'inquiétude curieuse, allant du simple « trouble » non verbalisé à la certitude d'avoir été grugé ? Le présent article, qui fournit un cadre d'interprétation à la relation de manipulation sur Internet, ne prétend pas fournir une réponse à cette question qui mériterait une étude approfondie.

Le spam, souvent analysé à partir de l'idée qu'il abuse de la « crédulité » de personnes vulnérables, peut ainsi être regardé comme un moyen d'abuser aussi l'*incapacité* de celle-ci *à réfréner* une excitation pour un inattendu heureux (une surprise miraculeuse). Il n'est ainsi pas de crédulité forte sans une indexation sur des dispositions ou des dispositifs d'excitation. Par ce processus, Internet participe d'une intensification de notre vie nerveuse, liée aux rencontres potentielles qu'il permet, et répond à un esseulement de certains individus et à une tendance à l'étiolement ou à la désagrégation de leurs sociabilités.

RÉFÉRENCES

AHMED, T. et OPPENHEIM, C. (2006), "Experiments to identify the causes of spam", *New information perspectives*, vol. 58, n° 3, pp. 156-178.

AOKI, K. (2005), "Communities of Practice and Organizational Analysis", in Iwauchi, R., Takahashi, M., Murata, K. et Aoki, K., *Post-modern Organization Theory*, Dobunkan, pp. 205-232.

ATTA, S. (2009), "Yahoo ! Yahoo !", in *Lawless and other stories*, Lagos, Farafina.

AURAY, N. (2010), «Les technologies de l'information et le régime exploratoire», in van Andel, P., Bourcier, D. (éds) *La serendipité dans les arts, les sciences et la décision,* Paris, Hermann, pp. 329-343.

BERG, S. (2009), « Identity Theft Causes, Correlates, and Factors: A content Analysis », in Schmalleger, F. & Pittaro, M. (eds), *Crimes of the Internet*, New Jersey Pearson Prentice Hall, pp. 225-250.

BOYER, P. (1992), *Tradition as Truth and Communication*, Cambridge: Cambridge University Press.

BRUILLART, K. (2009), « Worldwide Slump Makes Nigeria's Online Scammers Work That Much Harder », 7 août, *Washington Post*.

BRUNER J. (2002), *Pourquoi nous racontons-nous des histoires ?* Paris, Retz.

CARDON, D. (2010), *La démocratie Internet. Promesses et limites*, Paris, Seuil.

CEFAÏ, D. (2002) « Qu'est-ce qu'une arène publique ? Quelques pistes pour une approche pragmatiste », in Cefaï D. et Isaac J. (éds), *L'Héritage du pragmatisme. Conflits d'urbanité et épreuves de civisme*, La Tour d'Aigues, Éditions de l'Aube.

CHATEAURAYNAUD, F. (2004), « L'épreuve du tangible. Expériences de l'enquête et surgissements de la preuve », in *La croyance et l'enquête. Raisons pratiques*, vol. XV, Paris, EHESS.

CHÂTEAURAYNAUD, F. (2007), "Les asymétries de prise. Des formes de pouvoir dans un monde en réseau", HAL (archives ouvertes en sciences humaines et sociales), halshs-00111674.

CLÉMENT, F. (2005), *Les mécanismes de la crédulité*, Droz, Genève.

CONEIN B. (2007), « Schémas de groupe, action conjointe et cognition sociale : l'hypothèse simmelienne », *Intellectica*, n° 2-3, pp. 46-47.

CORCUFF, P. (2010), « Défiance moderne, théories du complot et critique radicale », *Médiapart.*

DE BLIC, D., et LEMIEUX, C. (2005), « Le scandale comme épreuve », in *Politix*, vol. 71, n° 3, pp. 9-38.

DE BROSSE (2008), « ID theft victim becomes pawn in dating scam », 6 avril, *Dayton Daily News*.

DIXON R. (2005), « Nigerian Cyber Scammers », 5 avril, *L.A. Times*.

ESQUERRÉ, A. (2009), *La manipulation mentale. Sociologie de sectes en France,* Paris, Fayard.

FAVRET-SAADA, J. (2001), *Les mots, la mort, les sorts*, Paris, Gallimard.

FINCKENAUER (2007), *Mafia and Organized Crime*, Oxford: Oneworld Book.

FROISSART, P. (2007), « Buzz, bouffées d'audience et rumeur sur Internet ». *Médiamorphoses*, n° 21, pp. 81-87.

GENSOLLEN, M. (2006), « Communautés en ligne, échange de fichiers et partage d'expériences », *Esprit*, n° 154.

GOFFMAN, E., (1991), *Les cadres de l'expérience*, Paris, Éditions de Minuit.

GRIMES, G.A., HOUGH, M. C. et SIGNORELLA, M. L. (2007), "E-mail end users and spam: relations of gender and age group to attitudes and actions", *Computers in human behavior*, 23, pp. 318-332.

HARDVIG, J. (1991), "The Role of Trust in Knowledge", *Journal of Philosophy* 88(12), pp. 693-708.

HEIDERICH, D., 2004, *Rumeurs sur Internet*, Village Mondial.

HERRING, S. C. (2004), "Computer-mediated discourse analysis: An approach to researching online behavior", in S. A. Barab, R. Kling, & J. H. Gray (Eds.), *Designing for Virtual Communities in the Service of Learning*, New York, Cambridge University Press, pp. 338-376.

KAPFERER, J.-N. (1998), *Rumeurs. Le plus vieux média du monde*, Paris, Seuil.

KESSOUS, E., MELLET, K. et ZOUINAR, M. (2010), « L'*économie* de l'*attention* : Entre protection des ressources cognitives et extraction de la valeur », *Sociologie du travail*, vol. 52, n° 3, pp. 359-373.

LICOPPE, C. (2009), « Pragmatique de la notification », *Tracés. Revue de Sciences humaines* [En ligne], n° 16.

LOINTIER, P. (2008), *La criminalité informatique*, Paris, Dunod.

MOULIER-BOUTANG, Y. (2009), *Le capitalisme cognitif*, Paris, Amsterdam.

NEWMAN, G. & CLARKE, R. (2003). *Superhighway Robbery: Preventing E-commerce Crime*. Willan Publishing.

ORIGGI, G., 2007, *Qu'est-ce que la confiance ?*, Paris, Vrin, coll. « Champs philosophiques ».

POSLUNS, J. (2004), *Inside the SpamCartel*, London: Routledge.

SCHMALLEGER, F. & PITTARO, M. (Eds.), *Crimes of the Internet*, New Jersey: Pearson Prentice Hall, pp. 225-250.

SHAPIRO C. et VARIAN H.R. (1999), *Économie de l'information. Guide stratégique de l'économie des réseaux*. Bruxelles, De Boeck Université.

THÉVENOT, L. (2006), *L'action au pluriel*, Paris, La Découverte.