UNE HISTOIRE DU SPAM

Le revers de la communauté en ligne*

Finn BRUNTON

Traduction de Nonta LIBBRECHT-CAREY

* Ce texte est une traduction de l'article suivant : Brunton, Finn, "Constitutive Interference: Spam and Online Communities" in *Representations*, Vol. 117, Winter 2012, pp. 30-58. Le début du texte a été légèrement coupé.

 doi: 10.1525/rep.2012.117.1.30

DOI: 10.3917/res.197-198.0033

« SPAM », « COMMUNAUTÉ » ET AUTRES LIEUX

Le mot « spam » a une étymologie instable et mouvante qui reflète, en négatif, celle du mot « communauté » : le premier terme est péjoratif et abusif tandis que le second est persuasif et vaguement utile [1]. Tout commence par un sketch des Monty Python des années 1970, dans lequel des Vikings polluent la conversation d'autres personnages en chantant « spam, spam, spam » dans un restaurant. Ce sketch a été rejoué à l'infini dans les premiers forums en ligne, notamment parce qu'il se prêtait bien à une reproduction automatique et qu'il était un moyen efficace d'énerver les autres en prenant assez de place sur leurs écrans pour remplacer la conversation en cours [2]. Le terme en est venu à désigner de nombreuses formes d'activités indésirables dans le réseau, de la génération accidentelle de contenus suite au dysfonctionnement d'un algorithme à l'excès de contenus postés par un autre utilisateur ; de la simple

---

1. Les recherches et la rédaction de ce projet ont été financées par des bourses d'Air Force Office of Scientific Research: Multidisciplinary University Research Initiative (ONR BAA 10-002), National Science Foundation: Privacy, Obligations, and Rights in Technologies of Information Assessment (ITR-0331542), et National Science Foundation: Cyber Trust-Medium (CNS-0831124). Je les remercie de leur soutien. Mes conversations inspirantes avec Gabriella Coleman, Erica Robles et Alexander Galloway, les commentaires bienveillants et rigoureux des éditeurs de Representations ont grandement contribué à améliorer cet article. J'aimerais aussi remercier Helen Nissenbaum et Mario Biagioli pour la constance avec laquelle ils m'ont fourni une aide, des encouragements ainsi qu'un aiguillage exemplaire, sans lesquels cet article n'aurait pu voir le jour.

2. Le spam est présenté dans de nombreuses étymologies populaires du mot « chat », par exemple celle de James Parry : « À cette époque, nombreux étaient ceux qui, ne sachant pas comment lancer une conversation, tapaient les paroles de leurs chansons préférées ou, à l'instar des gens d'écoles d'ingénierie informatique comme [le Rensselaer Polytechnic Institute], récitaient mot à mot des sketchs entiers des Monty Python. Parmi ceux-ci, "spam, spam, spam, spammity spam" étaient particulièrement populaires, car il suffisait de l'écrire une fois et de taper sur la touche "flèche vers le haut" pour le répéter. Le "spamming" était donc le fait de submerger un chat avec ce genre de boucan. » James Parry, message dans le fil de discussion « Totally Spam? It's Lubricated » sur alt.religion.kibology, 2 septembre 2003, http://groups.google.com/group/alt.religion.kibology/msg/a89af63f065a35da?hl=en&dmode=source&pli=1, consulté le 27/04/2016.

apparition d'attitudes commerciales dans une société théoriquement neutre ou civile à la domination du discours en ligne par des contenus générés automatiquement. Le terme a facilement gagné des modes d'activité très différents les uns des autres. Quand, en 1975, l'architecte réseau Jon Postel écrivait la RFC 706 « *Request for Comments* », littéralement : « requête de commentaires », intitulée « *On the Junk Mail Problem* » « Du problème du courrier-poubelle », il parlait des contenus « déviants ou […] simplement importuns » envoyés par des programmes dysfonctionnels sur le réseau – une panne purement mécanique se produisant parmi un groupe très restreint d'hôtes. Lorsqu'une erreur de programmation frappa une conversation Usenet en 1993 en envoyant des centaines de copies d'un message qui se rallongeait de manière récurrente, elle entra dans les annales du *Jargon File*, qui consigne les néologismes et l'argot du réseau, comme « ayant relevé du spam »[3]. Le terme pouvait d'ailleurs encore s'appliquer au discours humain : en 1994, dans son panorama pionnier de l'univers textuel collaboratif de LambdaMOO, Elizabeth Hess écrivait ainsi que « le spam désigne le fait de générer tant de textes que ce volume est odieux par lui-même, indépendamment de son contenu » (Hess, 2003). Une demande d'expulsion d'une utilisatrice de LambdaMOO soumise en 1994 fait ainsi état d'« un passé riche en comportements vindicatifs, paranoïaques et diffamatoires, en harcèlement, en mensonges et en triche, mais surtout d'une compulsion au spam » – non pas un discours commercial, mais « de longs laïus à demi-cohérents », c'est-à-dire un discours indésirable (Marvin, 1995 ; Dibbell, 1998, p. 100). Ces incertitudes sont également entrées dans le discours légal, comme on peut le voir dans l'affaire *CompuServe, Inc. contre Cyber Promotions, Inc.* : « La défense utilise le terme de "courrier électronique de masse", tandis que les plaignants utilisent le terme de "courrier électronique-poubelle". Dans le langage vernaculaire d'Internet, les courriers électroniques publicitaires non sollicités sont parfois appelés péjorativement "spam"[4]. »

---

3. Jon Postel, *Request For Comments*: 706 : « On the Junk Mail Problem », novembre 1975, http://www.ietf.org/rfc/rfc706.txt (consulté le 27/04/2016) ; pour le message se reproduisant automatiquement, voir Eric Raymond, « ARMM », dans le *Jargon File* (sans date, mais voir la dénomination et le texte proposés par Joel Furr dans le fil « ARMM: ARMM: >>>>Ad Infinitum » sur news.admin.policy le 31 mars 1993 : http://groups.google.com/group/news.admin.policy/msg/dc98a1f9c6a59477?hl=en), consulté le 27/04/2016, http://www.eps.mcgill.ca/jargon/jargon.html#ARMM, consulté le 02/05/2016.

4. *Compuserve v. Cyber Promotions, Inc.*, 962 F.Supp. 1015 (S.D. Ohio, 1997). Le jugement présente un remarquable moment de surréalisme légal avec une note de bas de page spécifiant que « ce terme est tiré d'un sketch joué dans l'émission de télévision britannique *Monty Python's Flying Circus*, dans lequel la répétition du mot "spam" dans le menu d'un restaurant est poussée à l'absurde ».

« Massif », « poubelle », « interminable », « importun », « agressif » par son contenu ou sa quantité : le « spam » est, à très peu de choses près, l'inverse parfait de la « communauté ». Ce terme négatif dans la langue familière ou spécialisée, qui a toujours une signification étendue et vague, couvre un large spectre de pratiques techniques et sociales, de motifs, d'incitations, d'acteurs et de cibles. Ce flou est très fertile : ces mots servent de supports pour quantité d'évolutions et de définitions, d'individualités ou de groupes, de marchés ou de valeurs non commerciales, de manières de vivre appropriées et justes. Alors que la « communauté » renvoie à notre capacité à nous rejoindre, à partager nos efforts, à compatir, *et cætera*, le « spam » est le monument toujours plus grand de nos défauts les plus banals : la crédulité, l'incompétence technique, la luxure (et la triste angoisse de l'impuissance masculine), la vanité et l'avidité devant les enjeux les plus mesquins. La communauté évoque ce que les gens ont de généreux, de compréhensif et de sociable, alors que le spam n'évoquera jamais que des pigeons, des criminels et des crétins.

Le spam, c'est l'histoire de l'ombre, l'espace en négatif, du concept de communauté en ligne. C'est aussi une force significative dans cette histoire, la mise à l'épreuve des limites, la provocation pour de nouveaux développements, l'échec permettant de définir le succès. Germant sous diverses formes dans tous les lieux où vient se focaliser l'attention d'un groupe – que ce soit sur un forum, dans un commentaire de blog, un groupe Usenet ou dans des zones où l'attention collective est plus diffuse, telles que les résultats agrégés par l'algorithme PageRank de Google ou l'espace des adresses e-mail personnelles –, le spam augmente les contradictions internes des communautés en ligne. La communauté virtuelle a une telle variété de formes d'expression et de programmes dans son sac qu'elle appelle des conversations, des débats et des clarifications, tant sur le nouvel ordre qu'elle produit que sur l'ancien ordre qu'elle perturbe ou rend obsolète, ainsi naît le spam qui vient interférer avec cette communauté virtuelle et révéler ses contradictions internes. Comme le dit Alexander Galloway, l'essor de la médiation en ligne et des communautés nous oblige à trouver une « nouvelle logique d'organisation », à défaut de quoi le fossé entre nos vieux modèles et les nouvelles formes ne cessera de se creuser et d'être plus difficile à supporter[5]. Cet écart est très évident dans les domaines qui sont structurés autour de la rareté ou de

5. Alexander R. Galloway, « Position Paper », *Exploring New Configurations of Network Politics*, 2010, http://www.networkpolitics.org/request-for-comments/alexander-r-galloways-position-paper.

la confidentialité des informations, comme le journalisme, l'édition de livres ou de musique, la diplomatie ou encore l'intimité sélective du quotidien, ce qu'Helen Nissenbaum nomme l'« intégrité contextuelle », où l'on opère une nette séparation entre les amis, la famille et le travail (Nissenbaum, 2010). À travers un cas fondamental et actuel – même s'il est négatif –, le spam est un indicateur de cette nouvelle logique d'organisation en acte, et il redéfinit notre compréhension de la « communauté » en ligne, montrant son fonctionnement et ses paradoxes.

[…]. Comme le modèle du « public » de Dewey, créé par un « intérêt commun » dont l'existence consiste principalement en une capacité à « se localiser et s'identifier », à s'unir et à concentrer de l'attention, des votes et de l'argent afin de lutter contre ce qu'il perçoit comme une conséquence négative, le spam produit des publics réactionnels (Dewey, 2010[6]). Soudainement obligés d'être conscients des moyens de leur propre existence et de créer de manière délibérée des mécanismes qui brouillent les frontières entre technique, social, politique et juridique, ces publics réactionnels doivent se gérer en tant qu'infrastructures et, au passage, répondre à de grandes questions : Au nom de qui ? Selon les critères de qui ? Avec quelles méthodes ?

Oui, peut-être avez-vous bien une « communauté », avec tout le bagage émotionnel qu'implique ce terme où s'entrelacent les solidarités et les intérêts partagés, mais votre communauté est aussi un agencement particulier de matériel et de logiciel. Elle a besoin d'électricité. Elle est faite de serveurs montés en *rack*, d'Apache et d'un logiciel d'interface forum. Peut-être vit-elle de revenus publicitaires ou du bénévolat ou bien des largesses d'une entreprise. Peut-être votre communauté appartient-elle à quelqu'un d'autre ou est-elle sujette aux lois de quelqu'un d'autre. On peut citer les exemples les plus récents et les plus importants de cette tension : Google et le gouvernement chinois, les réseaux sociaux et le gouvernement iranien, Facebook et la vie privée ou la question : « Un tweet peut-il être assujetti au droit d'auteur[7] ? » Peut-être que, comme GeoCities – ou Imeem, Lively, AOL Home-town, OiNK, et ainsi de suite dans la liste nécrologique –, votre communauté disparaîtra un jour, sans prévenir ou presque, avec son contenu généré par les utilisateurs et tout le reste. Or, avant qu'elle ne s'évapore comme un mirage suite à un changement

6. Dans l'édition en anglais, « into existence » : p. 126 ; « locate and identify » : p. 141.
7. Sur les nouveaux médias et l'Iran, voir Srebeny (2009) ; sur Facebook et la vie privée, voir Grimmelman (2009) ; sur Twitter et la propriété intellectuelle, voir Shinen (2009).

de stratégie commerciale, comment doit-elle se réglementer, se réguler et se maintenir, comment va-t-elle définir ses règles ? La gouvernance sur Internet est l'espace du *vraiment différent* (Lee A. Bygrave et Jon Bing l'avaient parfaitement montré dans *Internet Governance*, 2009) où les propriétés du réseau déterminent considérablement ce qui s'y échange[8].

Ces propriétés elles-mêmes peuvent tout aussi bien changer selon différentes échelles et populations, de machines et d'utilisateurs – le spam exige souvent les réponses d'un collectif, d'un « nous » qui peut tout aussi bien désigner « les quelques centaines de personnes sur le réseau » qu'une sensibilité politique vague d'internautes éparpillés sur des systèmes accueillant des millions de personnes dans le monde, voire même « les citoyens des États-Unis utilisateurs d'Internet ». Ces différentes échelles donnent lieu à différentes modalités d'organisation, de doléances, de corrections et d'invocation persuasive de la « communauté ». Cela suggère une comparaison avec l'histoire de la physique : nous pouvons établir une distinction entre l'échelle quantique, l'échelle atomique et l'échelle galactique parce que ces trois physiques obéissent à des types de lois très différents – l'élégante simplicité de la physique newtonienne s'arrête à la frontière entre les domaines atomique et subatomique, où l'étrangeté de la mécanique quantique prend le pas, et elle est subsumée à sa limite supérieure par l'échelle cosmique, encore plus élégante, qui permet de suspendre la chimie, l'électromagnétisme et leurs pairs pour ne plus travailler qu'avec la masse et la gravité. De même, le difficile point d'équilibre entre le groupe et les moyens lui permettant d'exister comme tel peut être atteint à toutes les échelles que l'on rencontre dans l'histoire du réseau, mais cet équilibre et ses modifications prennent des formes très différentes dans un petit réseau professionnel et dans un système public de grande ampleur ou selon que l'échelle est nationale ou internationale.

Les spammeurs pèsent simplement sur ce point d'articulation entre l'infrastructure et le concept de communauté, en l'exploitant sans relâche, en travaillant dans l'espace où nous sommes forcés de réfléchir à nos technologies, parce qu'elles sous-tendent la compréhension que l'on en a et l'usage que

8. Comme le disait Bryan Pfaffenberger (1996) au sujet de la liberté d'expression sur Usenet : « On ne peut pas expliquer la notion de liberté d'expression que l'on trouve aujourd'hui sur Usenet en l'assimilant à des traditions de liberté d'expression développées dans des contextes non technologiques ; à l'instar de la plateforme Usenet elle-même, cette liberté est un artefact qui s'est développé pendant que des groupes concurrents luttaient dans une nouvelle arène technologique. »

l'on en fait en même temps qu'elles en divergent. Cette tension est l'habitat naturel du spam. C'est là ce qui le distingue d'autres formes de criminalité informatique et c'est pourquoi il est particulièrement pertinent de parler de communautés virtuelles et réelles : les spammeurs prennent l'infrastructure des « bonnes choses » et la poussent ensuite à ses extrêmes. Le *spamming* est la forme hypertrophiée des technologies et des pratiques qui conditionnent précisément l'existence des communautés virtuelles et qui le combattent. C'est pourquoi il est si difficile à définir et à éradiquer et si précieux pour notre compréhension des réseaux numériques et des rassemblements qu'ils permettent. C'est ce fait-là qui rend le spam vraiment unique. […]

Alors que Google affine sa stratégie de blocage et d'exclusion des spammeurs publicitaires les plus déclarés, les spammeurs travaillent avec obstination et diligence à une ingénierie qui prend le contre-pied de ces nouvelles améliorations, trouvant de nouvelles manières de les contourner dans une relation co-constitutive, une vraie course à l'armement, que l'on peut observer tout au long de l'histoire des spammeurs et de leurs cibles[9]. Cette dynamique devient visible assez tôt dans l'histoire d'Internet. À chaque tournant, les spammeurs mettent en lumière les contradictions en les exploitant et en soulevant des questions qui auraient sans cela été ignorées, en particulier celles de savoir qui ou quoi appartient à la conversation sur le réseau et quelles sont les limites concrètes de la communauté. Le spam pose des questions et exige des réponses, transformant les usagers en publics et forçant des « communautés » inclusives à se former et à se distinguer. Les spammeurs et leurs outils jouent un rôle majeur et sous-estimé dans la transformation des groupes qui utilisent ces technologies – de la communauté au public, puis du public aux citoyens –, dans la

9. Voir, par exemple, la présentation de l'algorithme de Google comme étant en partie une manière pour prévenir le détournement du système : « Les moteurs de recherche automatiques qui reposent sur l'association de mots clés rendent en général trop de résultats de mauvaise qualité. Pour ne rien arranger, certains publicitaires tentent d'obtenir de l'attention en adoptant des mesures visant à fourvoyer les moteurs de recherche automatiques… Il arrive souvent que les "résultats-poubelle" submergent tous les résultats qui auraient été susceptibles d'intéresser l'utilisateur » (Brin et Page, 1998). Ou voir encore l'article de l'année suivante sur l'analyse des liens internet, qui est lié de près à celui-ci et dans lequel on voit le terme de « spam » remplacer celui de « junk » (« poubelle ») dans le vocabulaire spécialisé : « Les liens sur Internet représentent un soutien et une reconnaissance implicites du document visé… Plusieurs systèmes – comme HITS, Google et Clever – reconnaissent ce fait et s'en servent dans leurs recherches sur Internet. Plusieurs autres grands portails semblent aussi utiliser des statiques [*sic*] sur les liens, car, contrairement aux fonctions de classement qui reposent uniquement sur le texte, les statistiques sur les liens sont relativement plus difficiles à "spammer" » (Kumar *et al.*, 1999).

constante redéfinition de leurs conditions d'existence, comme de la relation qu'ils entretiennent avec les instances antérieures de pouvoir et de contrôle qui ne sont pas toujours compatibles avec les nouvelles logiques d'organisation.

L'évolution conjointe du spam, de la communauté et de la gouvernance (1971-2010)

L'histoire qui suit sera envisagée dans ses grandes lignes. J'ai l'espoir qu'elle fournira un panorama, vu de très haut, de la vie commune et des rapports complexes du « spam » et de la « communauté », ainsi que des pratiques de gouvernance qui ont évolué entre eux, à titre de fondations pour de futures études du spam. Chaque événement évoqué dans cette histoire pourrait faire par lui-même l'objet d'une étude enrichissante de l'évolution enchevêtrée de notre société de réseaux révélant des événements mondiaux, des fortunes faites et perdues, des inventions, des anti-inventions et des anti-anti-inventions. Collectivement, ces événements composent une histoire dans laquelle le spam fait toujours partie d'une conversation sur la « communauté », ses significations et ses limites.

1971-1994

Cette histoire commence simplement, longtemps avant l'avènement d'Internet, au Massachusetts Institute of Technology (MIT), en 1971. Celui-ci accueillait la plate-forme centrale du *Compatible Time-Sharing System* (CTSS – en français, « système accomplissant du temps partagé ») pour l'accès informatique à distance. De nombreux utilisateurs de terminaux distants – à peu près mille, à la fois au MIT et dans d'autres institutions – avaient accès à une unité centrale et pouvaient s'en servir pour faire tourner des programmes ; grâce aux travaux de Tom Van Vleck et Noel Morris, deux programmeurs du MIT, les utilisateurs pouvaient aussi se servir d'une sorte de messagerie, un système permettant de transférer des fichiers vers des usagers choisis, qui précédait l'e-mail[10]. La commande « MAIL F1 F2 M1416 2962 » permettait d'envoyer un message à Van Vleck et « MAIL F1 F2 M1416* » permettait d'envoyer un

10. Tom Van Vleck, « The History of Electronic Mail », 2008, http://www.multicians.org/thvv/mail-history.html. L'essayiste et réalisateur de documentaires Errol Morris a mené plusieurs entretiens passionnants avec Van Vleck et d'autres personnes impliquées dans l'histoire du temps partagé et de la messagerie électronique : Errol Morris, « Did My Brother Invent E-Mail with Tom Van Vleck? » parties 1-5, *New York Times*, 19 juin 2011, http://opinionator.blogs.nytimes.com/2011/06/19/did-my-brother-invent-e-mail-with-tom-van-vleck-part-one/. Sites consultés le 27/04/2016.

message à tous les membres d'une équipe de recherche visée (dans ce cas-ci, l'équipe qui s'occupait du projet de programmation du CTSS en lui-même). Pour des raisons structurelles, les membres de l'équipe de programmation du CTSS avaient un privilège unique : ils pouvaient entrer la commande « MAIL F1 F2** » pour envoyer un message à tous les usagers du système CTSS. « J'étais bien mécontent, écrit Van Vleck, le jour où, probablement vers 1971, j'ai découvert qu'un membre de mon équipe [un administrateur système du nom de Peter Bos] avait abusé de son privilège pour envoyer un long message contre la guerre à tous les usagers du CTSS, qui commençait par : il n'y a pas de chemin vers la paix. La paix est le chemin. » Van Vleck lui a « fait remarquer que c'était inapproprié, ce à quoi il a répondu : "mais c'est important !" ». « Il n'y a pas de chemin vers la paix » est une citation du pacifiste chrétien A. J. Muste, un activiste qui luttait avec dévouement contre la guerre au Vietnam ; 1971, évidemment, était une époque de contestation de la collaboration entre l'armée et les universités, deux ans après la formation de l'*Union of Concerned Scientists* au MIT. Bos avait usé de son privilège en tant qu'administrateur système pour transformer ce médium théoriquement téléphonique de personne à personne ou de personne à un groupe en un système de diffusion d'une personne à toutes les autres personnes, transformant ainsi ce groupe de personnes utilisant la même unité centrale en une communauté politiquement engagée de personnes de mêmes opinions. Van Vleck et Morris avaient créé une solution élégante pour l'adressage de fichiers dans un ensemble de comptes informatiques en temps partagé, mais ils avaient aussi créé un public penchant fortement vers le groupe précis qu'un programmeur moralement passionné par la lutte contre la guerre aurait voulu atteindre et convaincre – des ingénieurs travaillant sur des contrats défense.

Cette histoire devrait être plus complexe : elle est à la fois celle d'un nouveau moyen de communication, d'un noble effort et de quelque chose d'effrayant. Mais la position de l'administrateur dans le système, avec sa maîtrise du code et ses privilèges d'accès permettant de le modifier, est celle du législateur, qui crée et supprime des comptes et modifie les capacités et la structure du réseau. Bien sûr, ces souverains sont à leur tour soumis à l'autorité des universités, des entreprises ou des gouvernements qui les emploient – un équilibre de pouvoirs souvent difficile.

Prenons un autre cas de « protospam », un message envoyé à des adresses ARPANET le 1er mai 1978, qui a lancé un débat dont les implications se font encore sentir. Cette dispute familiale parmi les Olympiens suggère

pourquoi nous sommes encore en guerre sur la plaine de Troie à ce jour. Les Olympiens : la liste des 593 adresses réceptrices de ce message publicitaire incluait ENGELBART@SRI-KL, Douglas Engel-bart, co-inventeur de la souris et personnage clé dans les interactions homme-ordinateur ; POSTEL@USC-ISIB, Jon Postel, un des architectes d'Internet, qui était pendant une période l'autorité en matière d'assignation des adresses IP ; FEINLER@SRI-KL, Elizabeth « Jake » Feinler, qui dirigeait le *Network Information Center* (NIC) et qui, par une décision directoriale, a créé la structure de noms de domaines en « .com », « .org », etc. [11]. Le message était une publicité pour les nouveaux ordinateurs réalisés par la Digital Equipment Corporation :

« Digital organise une présentation des tout nouveaux membres de la famille DECSYSTEM-20 » [12].

Les ordinateurs de la gamme DECSYSTEM-20 étaient les premiers à être vendus en intégrant un support pour se connecter à ARPANET ; il était évident que ce serait important pour les utilisateurs d'ARPANET. C'était précisément le groupe des personnes qui désiraient avoir cette information.

Ce message mit en évidence une dissension au sein du concept de « communauté » dans le réseau, une division que Kendall saisit en distinguant la communauté en tant que « communication et intérêts partagés » – la communauté qui existe sous sa forme la plus simple comme marché et cible des produits, une structure institutionnelle dont les racines sociologiques sont dans le *Gesellschaft* – et la communauté de « relations et de valeurs », de « valeurs humaines profondes », du *Gemeinschaft* (avec tout le bagage que ces deux catégories apportent avec elles) (Kendall, 2011). La première de ces formulations, qui voulait que la communauté soit une « famille » d'utilisateurs au même titre que les DECSYSTEM-20 formaient une famille de machines, était sous-entendue dans la réponse adressée par le major Raymond Czahor à DECSYSTEM :

« C'était une violation manifeste dans l'usage d'ARPANET, car le réseau ne doit être utilisé que pour les besoins officiels du gouvernement américain. »

---

11. Du fait de l'incompétence technique des expéditeurs, une grande partie des destinataires figurant sur la liste n'a jamais reçu ce message.
12. Brad Templeton, « Reaction to the DEC Spam of 1978 » (sans date), http://www.templetons.com/brad/spamreact.html, consulté le 27/04/2016.

C'est un arrangement contractuel et industriel, fondé sur la complémentarité des travaux. ARPANET ne doit pas être utilisé pour des publicités extérieures, car son attention, sa bande passante et son matériel sont la propriété des institutions qui l'ont créé, pour leurs communications et leurs intérêts partagés.

Une position plus nuancée, ouvrant la possibilité de valeurs aussi bien que d'intérêts partagés, fut exprimée au sein de la base d'utilisateurs dans un post d'Elizabeth Feinler daté du 7 mai qui faisait suite au communiqué officiel de Czahor. Elle commençait par cadrer la conversation d'un avertissement liminaire : « Ces commentaires sont les miens. Ils ne constituent d'aucune façon un message officiel de la *Defense Communication Agency* ni du NIC. » Si le réseau officiel était, de fait, strictement réservé à l'usage du gouvernement, toutes les personnes impliquées l'utilisaient au travers de leurs titres officiels, mais il y avait deux réseaux et elle – qui était une administratrice occupant une position cruciale dans le réseau de machines et de protocoles supervisés par le ministère de la Défense – écrivait à titre personnel sur le réseau non officiel, celui des utilisateurs des machines, dont la vie sociale autorisait les correspondances privées, les jeux d'aventure textuels, les faire-part de naissance et de mariage, ainsi qu'une conversation à long cours sur la science-fiction.

> « Le message officiel, écrivait Feinler, nous a demandé (« nous », les utilisateurs du réseau) de gérer le problème nous-mêmes. Je pense personnellement que c'est raisonnable et que nous devons coopérer, sans quoi nous serons encombrés de contrôles qui gêneront tout le monde. »

Le « message officiel » qu'elle avait distribué à la demande de Czahor est distinct du groupe, « "nous", les utilisateurs du réseau », auquel elle se trouve également appartenir. La teneur de son message est univoque : trouvons un accord et réglons cela nous-mêmes et, de cette façon, nous pourrons maintenir notre part du réseau relativement libre de « contrôles qui gêneront tout le monde ». Les utilisateurs veulent-ils vraiment inviter les autorités sur leur réseau ? Pour emprunter un terme à la typologie des réactions aux inconduites en ligne dressée par Julian Dibbell, Feinler proposait une solution parlementaire, générant une structure de règles internes servant d'intermédiaire entre le « nous » et ce qu'elle appelle « les pouvoirs en place » – nous gouverner nous-mêmes dans la forme d'un compromis avec notre contexte général et prévenir de nouvelles incursions dans notre espace (Dibbell, 1993).

Ce caractère de compromis fut amplifié par la réponse de l'éminent Richard Stallman, RM@MIT-AI, possiblement celui qui a joué le plus grand rôle dans la création du mouvement des logiciels libres :

> « Il vient d'être suggéré que nous nous imposions les exigences de quelqu'un d'autre parce qu'il POURRAIT sinon nous les imposer… je doute que qui que ce soit puisse efficacement de l'extérieur forcer un site à s'imposer une censure si les personnes qui sont à l'intérieur ne sont pas fondamentalement convaincues de son utilité. »

Stallman présente un argument anarchiste sous sa forme la plus basique – « anarchiste » au sens de Dibbell : non pas un plaidoyer en faveur de la publicité, du spam ou du laissez-faire comme tel, mais en faveur de normes et de valeurs autoréglementées émergeant du réseau et appliquées par les « utilisateurs du réseau », plutôt que d'être importées, imposées ou médiatisées par le contexte du réseau. C'est de l'anarchisme au sens de Kropotkine, où la « loi coutumière », les normes et les lois qui se développent parmi « les membres d'une tribu ou d'une communauté » maintiennent « des relations cordiales » et fonctionnent de manière d'autant plus souple et optimale qu'elles ne subissent aucune intervention extérieure (Kropotkine, 2010). Ce qui pose la question de savoir « ce que doit inclure le "auto" de l'autorégulation » – uniquement le corps des utilisateurs ou aussi les fournisseurs d'accès à Internet (FAI), les entreprises intéressées et les gouvernements nationaux (Monroe et Verhulst, 2005) ? Aussi sûr que la pluie s'infiltrera dans un toit vétuste, les spammeurs pénétreront dans ces espaces par définition problématiques s'ils y trouvent quelque attention à saisir, travaillant dans les angles morts que génèrent les arguments sur la régulation, où la liberté, la confiance accordée aux utilisateurs et les domaines de réglementation croisent des technologies de reproduction et de transmission au pouvoir inouï. C'est là que les anti-spammeurs se regroupent pour les confronter.

C'est ici qu'intervient un changement d'échelle radical : on passe d'un réseau pouvant être représenté par un diagramme sur une simple feuille de papier et dont la majorité des usagers se connaissent personnellement, à une toile internationale reliant des milliers de serveurs et des millions d'usagers [13].

---

13. Pour un panorama passionnant des premières évolutions de Usenet, comprenant les questions de contrainte sociale (*flaming*) et les problèmes associés au fait d'en tirer profit, au niveau social et au niveau des infrastructures, voir Henry Edward Hardy, « The Usenet System », ITCA [International Teleconferencing Association] Yearbook, 1993 (McClean, Virginie, 1993), pp. 140-151; disponible en ligne sur http://internet.eserver.org/Hardy-Usenet-System.txt., consulté le 27/04/2016.

Le 27 mai 1988, dix ans presque jour pour jour après le message de Feinler, en réponse à un message de protospam envoyé sur Usenet par « Jay-Jay »/« JJ », un utilisateur postait le brouillon d'une lettre adressée aux *US postal authorities* et ajoutait en commentaire : « Ceci dit, j'ai peur que [l'envoi de cette lettre] n'ouvre une monstrueuse boîte de Pandore à une échelle que l'enjeu ne saurait justifier[14]. » Bien qu'elle fût fortement contestée, il existait encore une notion partagée voulant que la réglementation soit assurée par un « soi » représentant les usagers du réseau, organisés en une communauté unie et déclarée, et non par leurs gouvernements putatifs. « JJ », le pseudonyme utilisé par un dénommé Rob Noha pour cette petite escroquerie à la charité, avait rendu la situation plus complexe. Dans les cas d'inconduite précédents, les personnes ayant été importunées pouvaient simplement se tourner vers le pouvoir souverain de l'administrateur réseau de l'école ou de l'entreprise de la personne incriminée. L'administrateur pouvait alors évaluer la situation et sermonner le malfaiteur ou l'exclure du réseau. Or Noha, en postant sa supplique sur tout le réseau Usenet (« Étudiant Pauvre a besoin de Votre Aide ! »), utilisait l'adresse e-mail JJ@cup.portal.com. Portal.com, l'entreprise Portal Information Network, était l'une des premières entreprises privées à proposer un accès à Internet à ses clients par abonnement, alors que l'accès à Internet avait été jusqu'alors offert aux étudiants et aux employés par leurs écoles et leurs entreprises, ce qui rompait un élément clé de l'accord social tacite. À tous points de vue, l'acte de Noha était lié de manière perturbante au contexte extérieur des systèmes postaux, des devises et des entreprises : les administrateurs système avaient-ils un devoir de loyauté envers un consensus rudimentaire de « démocratie par le bas » ou envers les entreprises qui les employaient – elles-mêmes inféodées à leurs actionnaires et à leurs clients (Pfaffenberger, 1996) ? Usenet était le théâtre d'un débat houleux sur la liberté d'expression dans lequel la question de la gouvernance devenait toujours plus chargée : était-ce là une forme d'expression digne d'être défendue[15] ?

La réaction parlementaire à Noha dut faire face à quelques-unes des questions très réelles de gouvernance et de communauté que nous évoquions précédemment : qui voudrait en référer au gouvernement territorial ? Pouvons-nous

14. Matthew P. Wiener, message posté dans le fil « Nebraska Letter » sur news.misc le 27 mai 1988, http://groups.google.com/group/news.misc/browse_thread/thread/c7b4c158caa1f579/b13590445e1fba94, consulté le 27/04/2016.

15. Pour une analyse détaillée de la politique et des technologies de la liberté d'expression sur Usenet, couvrant entre autres le rôle des administrateurs système et le problème du spam, voir *ibid.*

nous administrer nous-mêmes ? Et qui sera en charge de ces décisions et de leur application ? (« En fait, plus précisément, qui voudrait vraiment que le FCC ou l'U.S. Mail viennent fouiner dans Usenet pour trouver un moyen d'utiliser ces posts dans un tribunal et, accessoirement, voir s'ils ne devraient pas exercer un contrôle plus visible sur un système de communication souterrain aussi visible que Usenet ?[16] ») Pour reprendre à nouveau un néologisme de Dibbell, il y avait une frange « technolibertarienne » qui proposait que tout ce bazar social soit mis de côté au profit du « déploiement, en temps et en heure, d'outils logiciels défensifs » – nul besoin du ministère de la Justice ni d'une quelconque Chambre étoilée de Usenet si vous avez une bonne technologie de « killfiling » (sélections de contenus à supprimer) pour masquer les messages indésirables[17]. Nombreux étaient de l'avis de rendre le travail des administrateurs de Portal.com si désagréable qu'ils finiraient par adopter les mesures de contrôle qui s'imposaient. Ce que, sous un bombardement de messages, ils finirent par faire, mais d'une manière complètement inédite :

> « Nous avons reçu un certain nombre de requêtes concernant JJ… S'il vous semble que ce sont là les questions brûlantes de notre époque, vous voudrez sûrement appeler JJ vous-mêmes. Vous pouvez le contacter aux coordonnées suivantes : Rob Noha (alias JJ) 402/488-2586. Si vous voulez un Internet bien réglementé, débrouillez-vous[18]. »

L'acte, et plus particulièrement ses conséquences, étaient prophétiques. La réaction sociale antispam, qui connut ses vrais débuts avec les posts venant de Portal, avait bien des caractères d'un groupe d'autojustice : elle était organisée par des volontaires, contrevenait parfois à la loi et avait pour but explicite de punir les mauvais acteurs contre lesquels « [les autorités] ne pouvaient rien » (pour citer les communications officielles entre Portal et la police)[19]. Ceci dit, l'analogie avec un « groupe d'autojustice » est mauvaise en un sens,

---

16. Bob Webber, message posté dans le fil « FCC? U.S.Mail.? (Re: J J's Revenge-Part II) » sur news.admin, 1er juin 1988, http://groups.google.com/group/news.admin/msg/a702f4908ded4c89?hl=en, consulté le 27/04/2016.
17. J. Dibbell, « A Rape in Cyberspace », http://www.juliandibbell.com/texts/bungle_vv.html, consulté le 27/04/2016.
18. Service consommateur de Portal Communications, message posté dans le fil « JJ's posting » sur news.sysadmin, 27 mai 1988, http://groups.google.com/group/news.sysadmin/msg/d8aed91249879fcf?hl=en, consulté le 27/04/2016.
19. Service consommateur de Portal Communications, message posté dans le fil « A Note From Portal Regarding the 'JJ' Incident » sur misc.misc, 1er juin 1988, http://groups.google.com/group/misc.misc/msg/b44db800c9cc7d0a?hl=en, consulté le 27/04/2016.

car ils n'ont jamais basculé dans la violence directe. Leurs méthodes relevaient de la méchante farce, du chahut, de la raillerie : appels en PCV à toutes heures, « fax noirs », commandes de pizzas à régler à la livraison, expédition de colis en contre-remboursement, e-mails grossiers et injurieux, exploits informatiques illégaux, harcèlement des parents, des collègues et des amis du malfaiteur. Les spammeurs présumés étaient poursuivis en permanence par un nuage de menaces, de *trolling*, d'insultes et autres abus qui étaient comme le reflet de leurs infractions aux mœurs du groupe avec toute la rudesse que permettait la technique. Cette réaction s'apparentait beaucoup à une autre forme d'autojustice, symbolique et collective, appelée charivari.

« Un couple marié qui n'avait pas eu de grossesse depuis un certain temps, écrivait Natalie Zemon Davis (1983) dans *Le Retour de Martin Guerre*, était une cible parfaite pour le charivari… Les jeunes hommes qui pratiquaient l'escrime et la boxe avec Martin durent s'assombrir le visage, s'accoutrer de vêtements de femmes et se réunir devant la maison Guerre, battant des fûts de vin, sonnant des cloches et faisant bruire leurs épées. » La pratique était dirigée contre tout ce que la communauté trouvait contre nature, comme les mariages entre jeune et vieux, les veuves se remariant avant la fin de la période de deuil, l'adultère et la violence domestique excessive. « Avec des bouilloires, des pelles à braises et des pinces, dit un texte hollandais, la populace se rue vers la maison du coupable, devant la porte duquel résonne une musique dont une vie entière ne suffit pas pour étouffer l'écho » (Palmer, 1978).

[…] C'est aussi ainsi que fonctionne le charivari dans notre cas : « Rob Noha / 8511 Sunbeam Lane / Lincoln, NE 68505 /(402) 488-2586 / Les annuaires téléphoniques sont des choses formidables », écrivait un utilisateur deux jours après que Portal ait posté le nom et le numéro de téléphone de Noha. « Est-ce que quelqu'un de Lincoln peut passer par chez lui relever l'immatriculation de sa voiture ? » Aussitôt, la foule se disperse « comme le vent mourant dans les branches » : le charivari est réactionnel, ne présentant pas de plan d'action arrêté au-delà de l'humiliation publique du malfaiteur, il meurt aussi vite qu'il s'est formé [20]. Face à un antagoniste plus sûr de lui, ayant l'audace éhontée de la *chutzpah*, le charivari épuise vite son répertoire.

---

20. Pour d'autres projets visant à bafouer la vie privée et à produire collectivement une humiliation publique en ligne, avec toutes sortes d'approches, de visées et d'histoires, voir Dongxiao Liu, « Human Flesh Search Engine: Is It a Next Generation Search Engine? », *3rd CommunicationPolicy Research, South Conference*, Beijing, Chine, 2008, http://ssrn.com/abstract=1555438, consulté le 27/04/2016, ainsi que le cours donné par Gabriella Coleman

Six ans après l'affaire Noha, le 12 avril 1994, Usenet – dont la base d'utilisateurs s'était encore multipliée de façon spectaculaire – hébergeait le premier message dit « de spam », qui comprenait un élément foncièrement perturbant du point de vue du charivari : de véritables coordonnées de contact. Noha avait utilisé un pseudonyme et une boîte postale, alors que les coordonnées de contact impliquaient une certaine légitimité – il s'agissait en l'occurrence d'une publicité et il était donc évident que les auteurs du message espéraient pouvoir être contactés par des clients. Lawrence Canter et Martha Siegel étaient deux avocats spécialisés dans le domaine de l'immigration qui espéraient se faire de l'argent en présentant sous un faux jour les formalités à accomplir pour se présenter au tirage au sort de la loterie pour la *Green Card* américaine (un permis de travail). Ils ne ressentaient aucun besoin de se cacher, bien au contraire. « La liberté d'expression est devenue une cause que nous voulons défendre », disait Siegel dans un entretien donné au *New York Times*. « À titre personnel, je continue d'être consternée par le manque de respect pour la liberté d'expression dont fait montre cette poignée d'individus, qui prendraient le pouvoir sur Internet s'ils le pouvaient[21]. » Notez le changement d'échelle : la vive colère provoquée par la publicité émanait désormais d'une « poignée » d'utilisateurs, présentés comme des extrémistes au sein de l'environnement commercial et constitutionnel du « net », qui leur était désormais étranger. L'aspect fondamentalement douteux du projet des avocats – aucun immigrant n'ayant besoin de leur aide pour remplir les « formalités » nécessaires pour s'inscrire à la loterie de la *Green Card*, à laquelle une simple carte postale aurait suffi – était éclipsé par leur capacité à se faire de la publicité : oui, ils avaient bien posté une publicité, et ils en avaient tiré un contrat d'édition, une entreprise de marketing et, selon leurs dires, cent mille dollars en nouveaux clients pour leur entreprise. Ils parlèrent dans le *Times,* plaidèrent leur cause dans un livre : « Le seul point sur lequel les deux camps de la guerre des publicités en ligne sont d'accord, c'est qu'aucune loi n'interdit la publicité sur Usenet… À défaut d'arguments légitimes à opposer à ce que nous avons fait, la majorité de nos détracteurs ont décidé que c'était "malpoli". » La population d'Usenet se replia sur une pluie de courriers haineux,

---

au Goldsmith College de l'Université de Londres le 16 mars 2010 : « Old and New Net Wars over Free Speech, Freedom and Secrecy; or How to Understand the Hacker and Lulz Battle Against the Church of Scientology », Internet Archive, "Community Audio," 58:39, http://www.archive.org/details/coleman-scientology_versus_the_internet, consulté le 27/04/2016.

21. Laurie Flynn, « "Spamming" on the Internet », *New York Times*, 16 octobre 1994. http://www.nytimes.com/1994/10/16/business/sound-bytes-spamming-on-the-internet.html, consulté le 27/04/2016.

des appels téléphoniques malveillants (*phreaking*), des lettres au Conseil de responsabilité professionnelle, et cherchèrent à faire prévaloir leurs vues sur news.admin.policy (Canter et Siegel, 1994).

1994-2003

En fin de compte, Canter et Siegel ont payé professionnellement le prix de ce spamming d'avant-garde, mais la pratique explosait déjà. La première chose que les spammeurs vendaient était les outils et le matériel, les documents et les logiciels, qui leur avaient permis de devenir des spammeurs – aujourd'hui, une partie de l'économie des vastes réseaux d'ordinateurs infectés générant du spam, appelés « botnets », repose sur les logiciels utilisés pour construire le *botnet*, comme c'était le cas en 2010 avec l'affaire « Mariposa », dans laquelle les trois gestionnaires du système n'avaient que très peu de compétences en programmation[22]. Ce *business model* est une sorte de miroir en négatif de la Licence publique générale GNU (GPL), la licence *open source* de référence, qui exige qu'un programme utilisant du code *open source* soit lui-même *open source* : de même, les spammeurs rentabilisaient leur investissement initial en permettant à d'autres de spammer à leur tour – à l'instar des premiers prospecteurs qui pendant la ruée vers l'or firent fortune en vendant des pelles et des tamis à ceux qui espéraient faire fortune. Les programmes d'envois massifs de mails, les contrats d'hébergement spéciaux « blindés », les didacticiels, les bases de données d'adresses e-mail étaient les produits phares de l'époque (la base complète des adresses AOL, soit 37 millions de personnes, fut vendue pour 52 000 $, dotant son propriétaire d'un formidable trésor de cibles à spammer et d'un produit ayant une très forte valeur de revente). Sont venus s'ajouter depuis l'hébergement de blogs automatisé et les services de génération de texte, la production de comptes e-mails hébergés, toutes sortes de packages d'escroquerie publicitaire, des systèmes de *malwares* prêts à l'emploi, les abonnements à des services permettant de tromper les systèmes de détection des automates CAPTCHA, etc[23].

---

22. Sur la vente de matériel, de logiciels et d'expertise pour le spamming, voir par exemple les travaux du spammeur Davis Hawke tels qu'ils sont décrits par Brian McWilliams (2005). Sur le manque de connaissances des programmeurs du *botnet* « Mariposa », voir BBC News, « Spanish Police Arrest Masterminds of 'Massive' Botnet », 3 mars 2010, http://news.bbc.co.uk/2/hi/technology/8547453.stm, consulté le 27/04/2016.

23. Sur la vente des adresses AOL, (McWilliams, 2005, p. 223). Le monde des produits auxiliaires pour le spamming est vaste ; le lecteur curieux pourra s'initier en consultant Captcha King, http://www.captchaking.com/ ; l'équipe de pirateurs de logiciels travaillant sur demande chez Rent-a-Cracker, http://www.rentacracker.com/ (notez combien de leurs logiciels piratés servent au spam) ; et ListGrabber et AutoMail, http://www.egrabber.com/listgrabberstandard/automail.html, sites consultés le 27/04/2016.

La tension constitutive se retrouve à chaque étape : alors que le spam se propage sous l'effet combiné du partage de compétences et de l'expansion rapide des publics et des capacités techniques, la lutte antispam suit une même évolution. En 1996, fut votée à 451 voix contre 28 la création du forum news.admin.net-abuse.email (NANAE), pour discuter « de potentiels abus des e-mails… du *mail-bombing*, des attaques par déni de service, des « listserv bombs », des e-mails non sollicités ou indésirables, des listes d'adresses e-mail, des abus liés à ces listes, de l'envoi massif d'e-mails en général », et ainsi de suite dans la liste toujours plus longue des malversations [24]. Le forum NANAE combinait les dossiers et les savoir-faire des chercheurs-farceurs experts en charivari, les méthodes légales de plaintes et de demandes de recours développées par l'aile parlementaire, des propositions de solutions techniques émanant des technolibertariens (facturer les e-mails, développer de meilleurs logiciels pour les filtrer), des conversations entre des administrateurs systèmes bien informés et le commun des utilisateurs d'Usenet et de messageries excédés par le spam. Après l'affaire Canter et Siegel, un communiqué de presse rédigé et revu sur news.admin.misc tentait de décrire le « contrat social implicite » en ligne que rompaient les spammeurs. Le NANAE a rendu ce contrat explicite, contesté et indispensable : une question immédiate de survie portée par une équipe de volontaires qui réunirent leurs compétences [25]. Ils rédigèrent des modes d'emploi simplifiés d'outils – des commandes telles que « whois » et « traceroute » ou encore un art d'extraire, dans des en-têtes d'e-mails chargés de données, les indices permettant de retrouver la trace des spammeurs et de les dénoncer – aussi bien que des documents plus longs, comme le « FAQ alt.spam » (24 000 mots), véritables monuments dédiés à la répression du spam [26].

Tout cela s'accompagnait d'une profonde incertitude sur la gouvernance – pour qui, et par qui ? Les campagnes de spam comme celles de Noha et de Canter et Siegel avaient suscité diverses déclarations au nom des « usagers d'Internet » – mais, en 1996, comment ces termes auraient-ils pu ne pas être

---

24. Jani Patokallio, message posté dans le fil « Result: News.admin.net-abuseReorganization All Groups Pass », news.announce.newgroups, 9 novembre 1996, http://groups.google.com/group/news.announce.newgroups/msg/2f658897021a0a89?dmode=source, consulté le 27/04/2016.

25. « Sine Nomine », message posté dans le fil « Proposed Press Release, 2nd draft », news.admin.misc, 6 juin 1994, http://groups.google.com/group/news.admin.misc/msg/f4d20bfe170f5edd?hl=en, consulté le 27/04/2016.

26. Ken Hollis, « Alt.spam FAQ » (créé en 1995), http://gandalf.home.digital.net/spamfaq.html., consulté le 27/04/2016.

équivoques ? Était-ce au nom des usagers et des actionnaires d'AOL ? Ou des intérêts représentés par Ira Magaziner, le conseiller scientifique du président Clinton, qui avait fait comprendre à Jon Postel qu'Internet appartenait au gouvernement américain et devait devenir un moteur d'échanges commerciaux (Goldsmith et Wu, 2006) ? Ou était-ce seulement au nom de ceux dont Martha Siegel se moquait en les qualifiant de « zélotes aux yeux hagards qui voient Internet comme leur maison »[27] ? Alors que le contingent antispam rassemblait des outils gouvernementaux pour soutenir sa lutte, il était divisé par de sérieux débats quant à l'efficacité et à la légitimité d'une présence en ligne des gouvernements nationaux, et notamment de la loi américaine CAN-SPAM, qui avait été copieusement moquée[28]. Les publicitaires pouvaient s'offrir les services de lobbyistes pour rédiger des lois faisant d'Internet un espace plus accueillant pour eux ; en s'alliant avec l'État, les groupes de volontaires comme le NANAE pouvaient bien gagner une bataille, mais perdre la guerre – en contribuant à créer un réseau au sein duquel les petits spammeurs auraient disparu parce que des acteurs plus puissants se seraient assuré le monopole de l'attention, à l'instar du monopole de la violence wébérien[29].

En fait, au-delà des gouvernements territoriaux, le NANAE a longtemps servi de lieu recevant les doléances et de cour d'appel dans le monde du spam. La période qui s'étend de 1994 à 2003 peut être considérée comme la phase locale, pendant laquelle les spammeurs et les anti-spammeurs se connaissaient

---

27. Laurie Flynn et Martha Siegel, « "Spamming" on the Internet », *New York Times*, October 16, 1994, http://www.nytimes.com/1994/10/16/business/sound-bytes-spamming-on-the-internet.html, consulté le 26/04/2016.

28. « Vous devriez également lire le Titre 47 du *United States Code*, Section 227. Il y a une FAQ sur cornell.law.edu où vous pouvez trouver le texte de la loi… Sylfest nous dit que les Norvégiens doivent les rapporter par e-mail au groupe de travail national sur la criminalité économique, KOKRIM » ; Hollis, « *Alt.spam FAQ* ». Notons que ce document inclut non seulement des conseils pour utiliser la loi et dénoncer les fauteurs aux autorités, mais aussi de nombreuses critiques des problèmes posés par les lois antispam déjà en vigueur ou débattues.

29. Le programmeur Paul Graham saisit le problème fondamental dans l'un de ses essais sur le filtrage du spam : « Il est maintenant difficile d'entériner des lois antispam efficaces, car il y a un continuum de spammeurs qui va des (soi-disant) "marketeurs par e-mails autorisés par le destinataire", comme Virtumundo, qui envoient des e-mails non sollicités à des adresses qu'ils achètent auprès de sites peu scrupuleux de la vie privée de leurs usagers, aux charognards comme Alan Ralsky, qui envoient des e-mails non sollicités à des adresses cueillies sur des pages web, des chats et des forums… Les entreprises se plaçant vers le pôle le plus légitime du spectre font du lobbying pour obtenir des vides juridiques dans lesquels les charognards pourraient aussi se glisser » ; Paul Graham, « So Far, So Good », août 2003, http://www.paulgraham.com/sofar.html, consulté le 27/04/2016.

et restaient encore relativement accessibles malgré tous les subterfuges employés, surtout pour les glaneurs assidus du NANAE. De nombreux spammeurs tentaient encore de donner à leurs entreprises un vague air de légitimité et maintenaient une sorte de conversation captieuse avec le monde des anti-spammeurs. Dès qu'une législation et des textes légaux antispam furent disponibles, de nombreux spammeurs les incorporèrent à leurs messages pour donner l'impression qu'ils agissaient en conformité à la loi et dans les limites de leur droit. (Au bout d'un moment, David Sorkin, qui gérait le site spamlaws.com, fut obligé d'expliquer qu'il n'était pas responsable de l'apparition dans les messages de spam de nombreux avertissements s'accompagnant d'un lien dirigeant vers son site (McWilliams, 2005, p. 139)). En 1998, Sanford Wallace, le spammeur qui se trouvait derrière Cyber Promotions, Inc., et qui tentait alors de quitter l'industrie du spam, publia une lettre ouverte dans laquelle il présentait ses excuses au NANAE (« Vous autres êtes en train de GAGNER la guerre contre le spam. Mon combat est terminé. ») – une forme de repentir qui ne s'adressait ni à un juge ni à un rapporteur, mais aux personnes qui étaient à la fois le plus à même d'exercer une pression sur les spammeurs et sur leurs entreprises et les seules, avec les autres spammeurs, à en comprendre les tenants et les aboutissants [30]. Le spam devenait une activité solitaire.

Une autre composante, plus restreinte, de ces groupes de volontaires était formée de ceux qui luttaient contre le spam en recherchant une solution non pas sociale, mais axée sur la technique et les infrastructures. Les interventions des gouvernements étaient vouées à pencher en faveur des médias en place, et les processus manuels de traçage et d'attaque des spammeurs utilisés par le NANAE ne pouvaient pas suivre une telle charge. Les technolibertariens qui cherchaient des outils logiciels pour casser le modèle des spammeurs trouvèrent une solution avec les systèmes de filtrage bayésiens. Lancés par l'article « A Plan for Spam » de Paul Graham, paru en 2002, des filtres à spam nettement améliorés firent leur apparition. Ils reposaient sur la probabilité statistique que certains mots apparaissent dans le spam plutôt que dans les autres messages (Graham, 2002). Les spammeurs étaient déjà passés experts dans l'art d'envoyer des messages en provenance de fausses adresses et d'éviter dans le paratexte les diverses marques révélatrices du spam, mais

30. Tel qu'il est cité par J. Leader et d'autres dans le fil « I'm Out! » sur news.admin.net-abuse.email, 11 avril 1998, http://groups.google.com/group/news.admin.net-abuse.email/browse_thread/thread/db1ce802d66ec505/, consulté le 27/04/2016.

leur langage, qui combinait argumentaire de vente et demande d'argent, pouvait être retourné contre eux. Des termes comme « quoique », « ce soir » et « apparemment » indiquaient de manière très fiable un mail légitime, tandis que « Madame », « garantie » et « république » dénotaient le spam : à partir de ces distinctions, il était possible de concevoir de puissants systèmes de blocage. Combinée à l'adoption de nouvelles lois exigeant l'usage d'un vocabulaire réglementé, l'introduction de clauses de non-responsabilité et de notices légales dans les e-mails de « marketing en ligne » nouvellement autorisés, l'adoption des filtres bayésiens a transformé l'économie du spam. Les taux de conversion des messages de spam avaient toujours été épouvantablement faibles ; maintenant que la grande majorité des spams était bloqués avant même d'avoir rencontré les yeux d'un utilisateur, le problème devenait absurde. Plutôt que de s'orienter vers un domaine plus facile, comme tirer des revenus des pages AdSense de Google, les spammeurs spécialisés dans les e-mails adoptèrent un mode opératoire ouvertement criminel, abandonnant au passage la prétention d'appartenir à l'industrie légitime de la publicité : il leur fallait produire des volumes de messages beaucoup plus élevés qu'auparavant, avec des caractéristiques susceptibles d'échapper au filtrage, et, pour chaque message réussi, dégager plus d'argent qu'une simple vente de pilules pour maigrir à base de plantes (par exemple).

Le besoin d'échapper aux filtres donna lieu à l'un des chapitres les plus étranges de l'histoire du spam. Les spammeurs intégraient à leurs messages des extraits de texte glanés sur des sites appartenant au domaine public dans l'espoir de tromper l'analyse statistique des mots, générant ainsi un tsunami moderniste de textes générés automatiquement et débités en tranches qui n'aurait pas semblé déplacé chez Tristan Tzara ou Louis Zukofsky. Le monde quelque peu ésotérique du spamming de résultats de recherches – sur des pages web, puis sur des formats de contenus générés par les utilisateurs, tels que blogs, commentaires et wikis, pour donner une illusion de popularité et de pertinence pouvant fausser les pages de résultats des moteurs de recherche à l'avantage du spammeur – avait déjà créé ce que j'appelle le « texte biface », une page web conçue pour être lue de manière complètement différente par un humain et par l'algorithme de classement d'un moteur de recherche en ligne. La *lit spam* (la littérature du spam utilisée dans les e-mails de spam) a poussé encore plus loin cette double lisibilité, avec une coquille de littérature statistiquement improbable disposée autour d'un lien ou d'une pièce jointe s'offrant au clic de l'utilisateur curieux.

Ce qui suivait ce clic indiquait les finalités de ce spam nouvelle génération – un volume de messages beaucoup plus important et un retour sur investissement[31]. Quand le destinataire crédule ouvrait le lien dans son navigateur ou téléchargeait la pièce jointe, un *malware* commençait discrètement à ronger son ordinateur. Cet *exploit*, cette faille, mettait sa machine au service d'un utilisateur distant, lui faisant rejoindre les rangs d'autres machines au sein d'un « botnet ». Quand le propriétaire légitime d'un ordinateur intégré à un *botnet* voulait faire un tableau ou consulter une page web, l'ordinateur recevait l'ordre d'envoyer des salves de spam – dont du spam d'autopropagation, c'est-à-dire des messages adressés à tous les contacts enregistrés dans l'ordinateur et envoyés avec un lien vers le malware qui permettait d'intégrer au *botnet* les ordinateurs de tous ces contacts à leur tour. Les analyses du *botnet* Storm montrent quelque chose de l'ordre d'une usine linguistique sophistiquée, avec des systèmes de files d'attente permettant de répartir la charge de travail entre les *bots* (robots) disponibles, des modèles-types de messages de spam et des systèmes de variations linguistiques permettant de passer les filtres, des mécanismes de retour d'information permettant de supprimer les adresses mortes de la liste mère, et un rythme de production atteignant 152 messages par minutes par ordinateur en moyenne, heure après heure, jour après jour, sur un réseau pouvant intégrer des milliers ou même des millions d'ordinateurs infectés (Kreibich *et al.*, 2008). (De plus, tout ordinateur infecté par un *malware* a de fortes chances de l'être par plusieurs, qui coexistent tant bien que mal ou tentent de s'éliminer mutuellement. Un nouveau ver qui cherche à coloniser une nouvelle machine est doté d'un kit anti-*malware* lui permettant de se débarrasser de ses compétiteurs. La compétition, l'imitation, la duplication et le recopiage sont présents à tous les niveaux dans le spam, même à ce niveau de complexité et de sophistication.) Comme ils ne peuvent envoyer du spam que quand les ordinateurs-hôtes sont allumés, les *botnets* ont une sorte de pouls en phase avec la rotation de la Terre. Le début et la fin de la journée de travail, le lever et le coucher du soleil, créent le cycle circadien planétaire du spam (Dagon *et al.*, 2006).

La masse excessive d'ordinateurs compromis a entraîné d'autres effets : avec un tel système, vous pouvez faire beaucoup plus qu'envoyer du spam ou

---

31. Précisons, par souci de clarté, que bon nombre des technologies de *malware* décrites ici avaient été développées avant d'être utilisées par les spammeurs – il existe, par exemple, des documents sur les vers et la distribution des opérations informatiques datant de 1982 –, mais leur adoption à ce moment-là reflète un profond changement dans la pratique du spamming par e-mail.

récupérer des mots de passe et des numéros de cartes bancaires. Vous pouvez utiliser une partie de la puissance de calcul accumulée pour déchiffrer des codes et des systèmes de protection, ou bien, à partir de tous les ordinateurs infectés, envoyer de manière rapide et répétée des requêtes à un site web en particulier, de manière à surcharger sa bande passante et le forcer à quitter le réseau – une « attaque par déni de service distribuée » (DDOS) au moyen de laquelle il est possible d'extorquer de l'argent aux propriétaires de sites et réduire temporairement des détracteurs au silence.

2004-2010

La menace des *botnets* a rencontré un système de résistance tout aussi mondial et sophistiqué sur le plan des infrastructures. Prenons par exemple le cas de McColo, un service d'hébergement web basé dans le Colorado, havre notoire pour les systèmes de *command-and-control* nécessaires pour faire tourner les *botnets* : à sa fermeture en 2008, le volume mondial de spam fut divisé par plus de deux – du moins temporairement – pendant que les propriétaires de *botnets* cherchaient de nouveaux hébergeurs pour rétablir leurs systèmes de contrôle. Parmi les forces ayant permis la fermeture de McColo se trouvaient des journalistes, des experts en sécurité et les administrateurs des grands centres lui fournissant sa bande passante[32]. (Sa fermeture laissa une étrange zone morte dans l'espace des adresses Internet : le bloc d'adresses allouées à McColo s'était retrouvé sur trop de listes noires pour ne pas rendre des repreneurs méfiants, comme une maison entachée par un suicide ferait fuir des locataires éventuels[33].) En mars 2010, en collaboration avec le FBI aux États-Unis et la Guardia Civil en Espagne, un groupe d'experts en sécurité appartenant à divers organismes forma le Mariposa Working Group, en vue d'appréhender les contrôleurs d'un grand *botnet* répondant au nom de « Mariposa ». Comme le remarquent Bygrave et Bing, le concept même de gouvernance en ligne est « diffus » à l'heure actuelle, et de même les actions coercitives, avec leurs groupes de travail informels chevauchant plusieurs juridictions et domaines d'expertise, et leurs parfois étranges compagnons de route – ainsi les spécialistes en sécurité finlandais, les observateurs de l'OTAN et de l'ONU et

32. Brian Krebs, « Host of Internet Spam Groups Is Cut Off », *Washington Post*, 12 novembre 2008. Pour la reprise progressive du spam par e-mail, voir Brad Stone (2009), http://bits.blogs.nytimes.com/2009/03/31/spam-back-to-94-of-all-e-mail/, consulté le 27/04/2016.

33. Brian Krebs, « A Year Later: A Look Back at McColo », *Washington Post*, 11 novembre 2009, http://voices.washingtonpost.com/securityfix/2009/11/a_year_later_a_look_back_at_mc.html., consulté le 27/04/2016.

les fournisseurs d'accès estoniens que les attaques DDOS contre l'Estonie avaient réunis en 2007 – en fonction de l'étendue du problème (Bygrave et Bing, 2009, p. 2)[34].

Même si beaucoup de chemin a été parcouru depuis que Peter Bos diffusait son message de paix dans tous les terminaux du MIT, cette histoire raconte aussi une sorte d'interrègne, une transition d'une période où le contrôle était ouvertement exercé par les administrateurs systèmes, à une autre. Les administrateurs systèmes des premières années, les figures Gandalfiennes maintenant l'ordre dans leur domaine selon leurs lumières, ont laissé place à ce qu'Alan Liu appelle « un clergé de codeurs de *back-end* et d'intergiciels » ainsi qu'une petite élite d'analystes en sécurité, d'agents de l'État et de fournisseurs d'accès[35]. Les utilisateurs peuvent se réfugier dans des zones relativement protégées du spam que construisent les développeurs, comme Gmail ou Facebook. Leurs robustes systèmes de filtrage et de *community management* sont payés par les publicités et les données des utilisateurs – c'est-à-dire à l'aide de leur attention, sujet sur lequel nous reviendrons. À cet égard, le spam joue un rôle important dans la dérive vers les monopoles qu'identifiait Tom Wu : l'irritation qu'il provoque pousse les utilisateurs vers les espaces privés qui peuvent employer des spécialistes en sécurité et regrouper assez de données d'utilisateurs pour développer des filtres à spam efficaces.

Le spam demeure infiniment divers, prospérant dans les interstices des architectures techniques et des *business plans*. À l'heure où le marché du spam par e-mail est dominé par une petite famille de titans des *botnets* se disputant des parts de marché à l'échelle mondiale, des petites escroqueries germent au sein des nouveaux espaces sociaux centralisés, tels que Facebook, Twitter et divers services d'e-mails avec hébergement : convaincre l'usager trop naïf de cliquer sur un lien, utiliser les robots de Twitter pour re-tweeter automatiquement les posts de certains utilisateurs afin de prêter à leurs contenus une popularité et une importance qu'ils n'ont pas, usurper ponctuellement une identité en recopiant le compte public d'une personne, composer un message de détresse plausible et collecter les sommes transférées en urgence par ses

---

34. La « guerre d'Internet » en Estonie a constitué à un événement complexe dont l'histoire n'a pas encore été écrite en détail ; pour une vue d'ensemble, voir Gadi Evron (2008).
35. Geert Lovink, « Interview with Alan Liu », networkcultures.org, 28 février 2006, http://networkcultures.org/wpmu/geert/interview-with-alan-liu/, consulté le 27/04/2016.

proches [36]. Nous n'avons même pas abordé ici le monde prospère et complexe des « 419 », ces demandes frauduleuses d'avance censées couvrir les coûts de déblocage de comptes cachés contre la promesse d'une énorme récompense, qui sont à l'origine de récits de chaos dont l'action se déroule entre Accra, Lagos et Rotterdam (et même d'un sous-genre cinématographique de Nollywood, l'industrie du film nigériane). Nous avons brièvement survolé le monde publicitaire souterrain de l'optimisation des moteurs de recherche par les « chapeaux noirs » ou *Black hats*, qui relie des carrières de pierre chinoises à des wikis académiques non sécurisés en Europe. Il y aurait un livre à écrire sur la lutte épique qui a opposé les membres inscrits sur le site de petites annonces Craigslist aux spammeurs, lesquels ont transformé une population éparse de propriétaires de téléphones mobiles à la recherche de nouvelles sonneries en une armée en ordre de bataille pour corrompre des systèmes d'identification vocale. Pour l'heure, cette brève histoire ne fait qu'esquisser quelques contours de la réalité du spam et de la relation à la fois constitutive et fondée sur l'exploitation d'autrui que ce dernier entretient avec les concepts de communauté, de gouvernance et d'expérience collective en ligne.

CONCLUSION : PENSER ENSEMBLE LE SPAM ET LES COMMUNAUTÉS

En se promenant dans les collines au-dessus de Sausalito au début des années 1990, Howard Rheingold et John Coate discutaient des manières dont une communauté virtuelle pouvait mal tourner, se diviser et s'effondrer. « Il faut qu'un noyau de personnes croie *mordicus* à la possibilité d'une communauté », concluaient-ils, faisant écho malgré eux à la communauté de Dewey (1954) comme « objet de désir », à la croyance en l'existence d'un domaine où des publics concurrents pourraient trouver un équilibre. […] Mais alors, comment cette croyance va-t-elle prendre forme ? Comment gérer au quotidien une affaire de désir, une magnifique perspective, qui peut en un instant se retourner sur elle-même et exploiter tous ses points de défaillance ? Au

36. Concernant le retweeting automatique sur Twitter : Andrei Boutyline, échange personnel. (Notez que cette automatisation est distincte des pratiques de retweeting effectué par les personnes que Danah Boyd, Scott Golder et Gilad Lotan ont étudiées dans « Tweet, Tweet, Retweet: Conversational Aspects of Retweeting on Twitter », *Proceedings of the 43rd Hawaii International Conference on Social Systems* (HICSS 43), 2010, http://www.danah.org/papers/TweetTweetRetweet.pdf, consulté le 27/04/2016.) En ce qui concerne les escroqueries sur les réseaux sociaux, le cas typique de Rakesh Agwaral est analysé par Graham Cluley dans « See a Facebook Scam in Action », sophos4.com, 22 janvier 2009, http://www.sophos4.com/blogs/gc/g/2009/01/22/facebook-scam-actio/, consulté le 27/04/2016.

travers « de normes, d'un folklore, de modes de comportements acceptables qui sont communément adoptés, enseignés et valorisés », résumait Rheingold (1994, p. 54). Ces comportements, ces normes, leur application au quotidien, ajoutés à la croyance en une possibilité d'existence du groupe, constituent la part « communautaire » de la communauté virtuelle, un acte d'attention se soutenant par lui-même et se définissant sous la constante pression de forces internes et externes – une forme que Randall Collins (2000) nommait dans son analyse de l'histoire sociale de la philosophie un « espace d'attention », un graphe de liens entre personnes consentant à s'écouter mutuellement et à débattre. « Pourquoi est-ce qu'une personne voudrait en écouter une autre ? Quelle stratégie apportera le plus d'auditeurs ? », demandait Collins, qui s'interrogeait sur les raisons pour lesquelles des écoles de pensée et des conversations fleurissent et prospèrent et d'autres non. La première question est au cœur de la notion de communauté, la seconde est au cœur du spam. Il est difficile de répondre à la première autrement que par l'affirmation « chaleureusement persuasive » de l'intérêt qu'il y a toujours à discuter entre personnes, à apprendre d'autrui, à partager et trouver des terrains d'entente – la rhétorique de la communauté dans toute sa puissance émotionnelle. Il est facile de répondre à la deuxième si l'on n'exige pas trop du concept d'« auditeur » : user de tactiques pour accaparer l'attention, automatiser la production de contenus, réaliser des économies d'échelle et tendre le plus grand filet possible. Et pourtant, ces deux questions sont intimement liées – répondre à l'une, c'est définir l'autre en négatif.

Ce qui nous amène à ce qu'il y a de « virtuel » dans « communauté virtuelle », c'est-à-dire le matériel, le code et l'infrastructure, l'étoffe concrète dont sont faites nos expériences et nos discussions en ligne. Tout au long de l'histoire des spammeurs et de leurs travaux, nous avons vu des communautés – soit des normes, des folklores, des comportements acceptables, des lois, des publics intéressés et concurrents, des actes d'autodéfinition et de réflexivité – dans l'obligation constante de produire des arguments qualitatifs et normatifs à propos d'abus quantitatifs. Vous venez de suivre une étrange mise en perspective de l'histoire des réseaux numériques où le spam se trouve au centre plutôt que sur les bords. Poussons encore plus loin ce projet à contre-courant et concluons par un exercice de sublime technologique, comme il est habituel de le faire dans les histoires d'Internet – sauf que c'est le spam qui se révèle ici sublime, tout en éclairant pourquoi il a généré tant d'affirmations de la communauté. Et si le spam n'était pas l'antithèse des systèmes d'Internet, mais plutôt ces systèmes utilisés de manière optimale et maximale – pour une certaine valeur d'« usage » ?

Considérons le spam diffusé par e-mail ou « pourriel », ces millions de messages crachés par des milliers d'ordinateurs à travers le monde dans l'espoir qu'un nombre infime d'entre eux seront vus par une fraction négligeable des personnes qui y réagiront vraiment (et se feront voler leur numéro de carte bancaire) : oui, jour après jour, mois après mois, ces spams génèrent un gaspillage prodigieux, proprement titanesque, en temps, en bande passante, en espace disque. Les spammeurs rempliront à ras bord chaque canal disponible et utiliseront toutes les ressources exploitables – tous ces cycles d'unités centrales perdus alors que l'ordinateur a été laissé allumé le temps d'une pause déjeuner ou que l'on planche sur un document Word peuvent maintenant être utilisés pour envoyer des pourriels polymorphes, tous uniques, à un rythme de plusieurs centaines par minute. Tant de blogs, de wikis et autres espaces sociaux qui sont négligés : les commentaires automatiques postés par des robots vont un par un venir saturer l'espace du serveur, comme des bernaches et des moules zébrées s'agglutinent sur la coque d'un navire abandonné qui finit par couler sous leur poids. Les serveurs font exactement ce qu'ils sont censés faire pendant les attaques par déni de service (DDOS) : ils envoient des pages web à un tel rythme et dans de telles quantités qu'ils ne peuvent plus proposer ce service à qui que ce soit d'autre. Les spammeurs adoptent des systèmes de travail par micropaiement comme le « Turc mécanique » d'Amazon et des services de création de contenus comme Textbroker[37] pour le spam de moteurs de recherche, afin de tirer parti de la production de travailleurs éparpillés (Haughey, 2010). Sous quelque perspective théorique que l'on se place, ce sont des éléments centraux dans notre compréhension des médias numériques qui sont réappropriés et subvertis jusqu'à l'extrême par les spammeurs : capacité à automatiser, manipulation algorithmique, rédaction de scripts, savoir-faire en effets réseaux et en économies d'échelle, connectivité décentralisée et participation gratuite ou à très bon marché. D'un côté, l'usage des machines est maximisé. D'un autre côté, les humains, dont l'attention constitue, en fin compte, l'unique enjeu, la seule ressource précieuse de tous ces agencements, sont un facteur fastidieux et problématique, car ils sont toujours susceptibles de signaler une page de spam, de bloquer un commentaire ou de supprimer un e-mail – un facteur inévitable, mais énervant, comme la traînée en aérodynamique. Il s'agit donc d'une majestueuse machine mondiale conçue pour répondre à la question de savoir comment conquérir les espaces d'attention et obtenir « le plus d'auditeurs ».

37. Textbroker, voir : http://www.textbroker.com, consulté le 27/04/2016.

Ce panégyrique de la fonctionnalité pure a beau être complètement ridicule, il n'en reste pas moins vrai. Alors, sur quelles bases arrêter le spam ? En travaillant sur les cadres logiciels, légaux et communautaires, nous devons emprunter le langage confus, fragile, émotionnellement chargé et contingent de la communauté, le champ principalement rhétorique que Manovich (2001) appelle la « couche culturelle » – ou, comme me l'avait décrit un ingénieur réseau : « le dessus de la pile des protocoles – c'est-à-dire les gens ». On trouve dans le monde des jeux vidéo un sens distinct du terme « spam », mais qui illustre ces distinctions : il s'agit des expressions « *grenade spamming* » ou « *ship spamming* ». Le « *grenade spamming* » est une stratégie à l'efficacité optimale, mais qui pêche par sa grossièreté fondamentale et son manque d'imagination : au lieu de faire quelque chose d'intelligent, d'excitant ou de dangereux, le joueur se contente de lancer vague sur vague de grenades contre son ennemi. Cette stratégie peut permettre de gagner la partie, mais ce faisant, on passe à côté de l'intérêt du jeu. « L'intérêt du jeu » tient à une distinction particulièrement humaine : tout joueur sérieux utilisera des techniques similaires pour optimiser les actions de son personnage et le spamming au cours du jeu n'est qu'une manière plus extrême d'optimiser ses chances de gagner. C'est le point extrême du spectre, au-delà de la limite floue et subjective de l'amusement, où gagner de la manière la plus efficace, la plus directe et la plus facile suffit. À un moment donné du processus, du moins pour la plupart des joueurs, il y a toujours un détour esthétique qui se fait au détriment de l'efficacité totale. Le « *grenade spamming* » dénote l'idée qu'il y a quelque chose qui cloche dans l'approche purement fonctionnelle du jeu, que quelque chose de supérieur est à défendre et se joue à travers les défis variés du jeu et de l'amusement – « jeu » et « amusement » étant évidemment des termes aussi délicats et complexes que « communauté ».

Le spam nous mène au cœur du jeu, prend parti pour lui et détermine quel usage des machines convient à notre compréhension de la communauté ; il soumet nos multitudes numériques aux mêmes tourments que ces dernières avaient imposés à tous les ajustements du monde analogique. Le média numérique et les logiciels ont été comme l'étincelle qui a mis le feu aux poudres dans les débats immenses sur le droit d'auteur et la propriété intellectuelle – sur les moyens par lesquels notre culture est reproduite et transmise. Les infrastructures de dépôt de documents anonymes et de publication distribuée ont ouvert de graves questions sur le secret, le devoir d'alerte et la relation entre l'État et ses citoyens. Le cryptage et le commerce en ligne menacent régulièrement de semer le chaos dans les caisses publiques ; les systèmes monstrueusement

complexes utilisés pour la modélisation et l'analyse de risques financiers ont déjà apporté leurs lots de désordres. La liste pourrait s'allonger – et à chaque étape, des questions sont soulevées et des arguments sont avancés sur ce qui peut être, ce qui pourrait, ce qui devrait être fait. La vie privée, les relations sociales, l'économie, la politique, nos modes d'apprentissage, notre manière d'écrire ou de faire de l'art : que reste-t-il, qu'est-ce que nos dispositifs et nos compétences n'ont pas encore mis en situation de crise ?

Ainsi fonctionne le spam, comme éternelle limite au domaine du possible, tout en en disant long sur ce qui a été limité. Tracer ces interférences constitutives nous aide à comprendre ce à quoi en veut le spam, ce que montrent aussi bien les travaux de Charles Stivale (1997) sur l'« escalade » des débuts du spamming (de l'« espièglerie » à l'« ambiguïté », jusqu'au « pernicieux » que l'on observe dans les pratiques actuelles de *trolling*), que les travaux d'ethnographie de Jenna Burrell (2008) sur la manipulation de stéréotypes médiatiques par les spammeurs 419 en Afrique occidentale, ou encore les études regroupées par Jussi Parikka et Tony Sampson (2009), qui prônent l'abandon des catégories analytiques du normal et de l'anormal devenues inutiles dans un réseau aussi fondamentalement imparfait. Deux grandes conclusions peuvent être dégagées de cette esquisse du spam.

Peter Sloterdijk (2009) écrivait que l'emploi du gaz de chlore par les militaires à Ypres, en 1915, avait entre autres entraîné une demande d'« explication » de notre environnement, mettant subitement au centre des attentions le caractère fragile de l'atmosphère (ce que Latour, commentant l'événement, a pu appeler « matière à préoccupation ») : « le fait que l'immersion d'un organisme vivant dans un milieu respirable en arrive au niveau d'une représentation formelle, exigeant un nouveau niveau d'explication des conditions climatiques et atmosphériques nécessaires à la vie humaine ». L'histoire des théories de la guerre juste inclut les *inimici*, soit des figures de pirates, d'indigènes, d'anarchistes, de forces apatrides sans sénat ni trésorerie, avec lesquelles il est impossible de conclure des traités. Ennemis éternels du commerce, ils demeurent extérieurs à l'État et en définissent l'une des limites, là où une « finance extraordinaire » va être provisionnée pour pourvoir à la guerre contre cet « ennemi de tous », si étranger à notre logique opérationnelle (Baucom, 2010). Les spammeurs combinent les deux formes abstraites de ces deux événements : d'une part, le moment où nous prenons subitement conscience de l'environnement dans lequel nous évoluons et des systèmes dont dépend notre vie, et, d'autre part, la reconnaissance de nos limites et les efforts extraordinaires que nous devons

déployer pour clarifier qui nous sommes et comprendre comment nous nous représentons. Ce que les spammeurs rendent explicite n'est plus l'atmosphère terrestre ou les frontières de l'État, mais la réalité technique du réseau et l'espace de notre attention – le milieu ou plus exactement le temps que nous occupons en ligne (des machines et des protocoles susceptibles d'être exploités) et nos manières de nous y constituer comme sujets. La « communauté » en ligne ignore les accidents de la proximité et de la géographie ; ce que les spammeurs mettent en évidence au point d'en devenir exaspérants, c'est que la communauté est faite de temps, de notre temps bien humain – et de notre attention. Cette communauté de temps et d'attention remonte aux premiers ordinateurs partagés de J.C.R. Licklider (1988) : « J'étais l'une des très rares personnes à l'époque à passer quatre ou cinq heures par jour devant une console d'ordinateur. » Elle a traversé la période des MOOs et d'Usenet, quand on déplorait le gaspillage de bande passante et la lecture de textes indésirables et dupliqués, jusqu'aux sites actuels qui cherchent à capter l'œil dans les premières pages de résultats des moteurs de recherches, aux e-mails annonciateurs de désastres, d'aubaine soudaine ou d'un ami en difficultés. Il peut sembler exagéré d'associer le spam à l'histoire des armes chimiques et de la guerre sans limites, mais le spam pointe vers une question existentielle similaire, bien que quotidienne et dénuée de toute gravité martiale : notre attention, ce sont nos vies, nos jours et nos heures de veille si limités, et même si nous n'en sommes pas conscients, nous construisons notre communauté et notre culture en ligne par des actes de concentration – cliquer, lire, écrire. Les spammeurs exposent tous ces moments d'attention du quotidien, traités comme un butin dont il faut s'emparer.

Les spammeurs sont loin d'être les seuls dans cette entreprise. Les entités variées de la lutte antispam étaient toutes inquiètes de voir les gouvernements nationaux intervenir dans le débat, parce que ces derniers étaient susceptibles de neutraliser les spammeurs indépendants tout en permettant à des intérêts plus puissants et mieux établis de s'engager dans un « marketing en ligne » légitimé – un monopole de l'attention finalement vendu à ceux qui pouvaient s'offrir les services de bons lobbyistes. Aujourd'hui, les techniques de spam migrent vers des entreprises plus légitimes, comme les fermes de contenus visant à augmenter le nombre de pages vues, et viennent alimenter le lexique des « *personality spammers* », des gens un peu trop enclins à faire leur promotion ou à lire leurs propres écrits. Une grande partie de l'histoire du spam est faite de grosses ficelles pour obtenir un clic ou un regard. Elles sont le tout-venant des colporteurs et des escrocs. Bien que rudimentaires, elles ont

une visibilité salutaire, car elles montrent à la fois leur milieu et leur constitution. Une grande partie de la sociabilité en ligne prend désormais place dans des environnements beaucoup plus subtilement conçus pour capturer l'attention. Ces environnements mobilisent toute la machinerie du *community management*, de la *gamification*, de la *stickiness* (capacité d'un site à maintenir l'usager « collé » dessus), et des mesures précises d'audience (les « publics quantifiés »). Des stratégies sont déployées pour limiter les sorties du site, afin que nous restions toujours en interaction avec la plateforme, nous, nos minutes de concentration, et les revenus qui les accompagnent – sans oublier, bien sûr, les systèmes de modération et de signalement pour tenir à distance le spam, comme un quartier contrôlé par une organisation criminelle qui en aurait vidé tous les bandits et voleurs à la petite semaine. Le vingt et unième siècle voit ainsi naître une lutte fondamentalement politique pour l'attention, afin de déterminer ce qui est disponible, ce qui nous interpelle, qui nous écoutons, et la manière dont nos systèmes de médiation technique forment et orientent notre vigilance. Ridicules, ingénieux, désespérés et effrontés, les spammeurs ont été les pionniers – les prospecteurs voyous du grand agrégat de l'attention humaine bien avant que l'industrie lourde ne prenne le relais. L'histoire de nos rapports avec le spam ne nous montre pas seulement la « communauté » en train de se faire, mais aussi les débuts d'une politique de l'attention en ligne.

RÉFÉRENCES

BAUCOM I. (2010), « Financing Enlightenment, Part Two: Extraordinary Expenditure », in Clifford SISKIN, William WARNER (dir.), *This Is Enlightenment*, Chicago: The University of Chicago Press.

BRIN S., PAGE L. (1998), « The Anatomy of a Large-Scale Hypertextual Web Search Engine », in *Computer Networks & ISDN Systems*, vol. 30, n° 1-7, pp. 107-117.

BURRELL J. (2008), « Problematic Empowerment: West African Internet Scams as Strategic Misrepresentation », *Information Technology and International Development*, vol. 4, n° 4, pp. 15-30.

BYGRAVE L. A., BING J. (2009), *Internet Governance: Infrastructure and Institutions*, Oxford: Oxford University Press.

CANTER L., SIEGEL M., (1994), *How to Make a Fortune on the Information Superhighway: Everyone's Guerrilla Guide to Marketing on the Internet and Other On-Line Services*, New York, NY: Harper Collins.

COLLINS R. (2000), *The Sociology of Philosophies: A Global Theory of Intellectual Change*, Cambridge, Mass.: Belknap Press of Harvard University.

DAGON D., ZOU C., LEE W. (2006), « Modeling Botnet Propagation Using Time Zones », Proceedings of the 13th Annual Network and Distributed System Security Symposium (NDSS'06), http://www.isoc.org/isoc/conferences/ndss/06/proceedings/papers/modeling_botnet_propagation.pdf, consulté le 27/04/2016.

DAVIS N. Z. (1983), *The Return of Martin Guerre*, Boston, Mass. : Harvard University Press p. 21. Traduction française : *Le Retour de Martin Guerre*, Paris : Tallandier, 2008.

DEWEY J. (1954), *The Public and its Problems*, New York: Swallow.

DIBBELL J. (1993), « A Rape in Cyberspace: How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society », *Village Voice*, 23 décembre 1993.

DIBBELL J. (1998), *My Tiny Life: crime and passion in a virtual world*, New York: Holt.

EVRON G. (2008), « Battling Botnets and Online Mobs: Estonia's Defense Efforts During the Internet War », *Georgetown Journal of International Affairs* Hiver/Printemps, pp. 121-126.

GOLDSMITH J. L., WU T. (2006), *Who Controls the Internet? Illusions of a Borderless World*, Oxford-New York: Oxford University Press.

GRAHAM P. (2002), « A Plan for Spam », http://www.paulgraham.com/spam.html, consulté le 27/04/2016.

GRIMMELMAN J. (2009), « Saving Facebook », *Iowa Law Review*, vol. 94, pp. 1137-1206.

HAUGHEY M. (2010), « *Does Amazon Enable Comment Spam?* », in *wholelotta-nothing.org*, 22 février 2010, http://a.wholelottanothing.org/2010/02/does-amazon-enable-comment-spam.html, consulté le 27/04/2016.

HESS E. (2003), *Yib's Guide to MOOing: Getting the Most from Virtual Communities on the Internet*, Victoria, Canada: Trafford.

KENDALL L. (2011), Community and the Internet, *The Handbook of Internet Studies*, Chichester: Wiley-Blackwell.

KREIBICH C., KANICH C., LEVCHENKO K. BRANDON E., VOELKER G. M., PAXSON V., SAVAGE S. (2008), « On the Spam Campaign Trail », Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET '08), 2008, http://www.usenix.org/event/leet08/tech/full_papers/kreibich/kreibich_html/, consulté le 27/04/2016.

KROPOTKINE P. (2010), *La Morale anarchiste. La Loi et l'autorité*, Saint-Didier : L'Escalier.

KUMAR R., RAGHAVAN P., RAJAGOPALAN S., TOMKINS A. (1999), « Trawling the Web for Emerging Cyber-Communities », *Computer Networks: The International Journal of Computer and Telecommunications Networking*, vol. 31, n° 11-1, pp. 1481-1493.

LICKLIDER J. C. R. (1988), « Some Reflections on Early History », in A. GOLDBERG (dir.), *A History of Personal Workstations*, New York, NY: ACM Press, pp. 115-140.

MANOVICH L. (2001), *The Language of New Media*, Cambridge, Mass.: The MIT Press, p. 46. Traduction française : *Le langage des nouveaux médias*, Dijon : Les Presses du Réel, 2010.

MARVIN L. E. (1995), « Spoof, Spam, Lurk and Lag: the Aesthetics of Text-Based Virtual Realities », *Journal of Computer-Mediated Communication*, vol. 1, n° 2, http://jcmc.indiana.edu/vol1/issue2/marvin.html, consulté le 27/04/2016.

McWILLIAMS B. (2005), *Spam Kings: The Real Story Behind the High-Rolling Hucksters Pushing Porn, Pills, and %*@)# Enlargements*, Sebastopol, CA: O'Reilly, pp. 89 et 180.

MONROE E. P., VERHULST S. G. (2005), *Self-Regulation and the Internet*, The Hague, Kluwer Law International.

NISSENBAUM H. (2010), *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford, CA: Stanford University Press.

PALMER B. D., (1978), « Discordant Music: Charivaris and Whitecapping in Nineteenth-Century North America », *Labour/Le Travail*, vol. 3, pp. 5-62.

PARIKKA J., SAMPSON T. D. (2009), *The Spam Book: On Viruses, Porn, and Other Anomalies from the Dark Side of Digital Culture*, Cresskill, NJ: Hampton Press.

PFAFFENBERGER B. (1996), « "If I Want It, It's Okay": Usenet and the (Outer) Limits of Free Speech », *Information Society*, vol. 12, n° 4, http://www.ingenta-connect.com/content/routledg/utis/1996/00000012/00000004/art00002, consulté le 27/04/2016.

RHEINGOLD H. (1994), *The Virtual Community: Homesteading on the Electronic Frontier*, New York, Harper Collins.

SHINEN B. (2009), « Twitterlogical: The Misunderstandings of Ownership », 2009, http://www.canyoucopyrightatweet.com/, consulté le 27/04/2016.

SLOTERDIJK P. (2009), *Terror from the Air*, Los Angeles, CA: Semiotext(e).

SREBENY A (2009), « Thirty Years on: The Iranian Summer of Discontent », *Social Text* (2009), http://www.socialtextjournal.org/periscope/2009/11/thirty-years-on-the-iranian-summer-of-discontent.php.

STIVALE C. J. (1997), « Spam: Heteroglossia and Harassment in Cyberspace », in David PORTER (dir.), *Internet Culture*, New York: Routledge, pp. 133-144.

STONE B. (2009), « Spam Back to 94% of All E-Mail », *New York Times*, 31 mars.