Internet et les réseaux sociaux : outils de contestation et vecteurs d'influence ?

Nicolas Arpagian

Dans Revue internationale et stratégique 2010/2 n° 78 , pages 97 à 102
Éditions IRIS éditions

ISSN 1287-1672
ISBN 9782200926700
DOI 10.3917/ris.078.0097
Date de mise en ligne : 28/06/2010

Internet et les réseaux sociaux : outils de contestation et vecteurs d'influence ?

Nicolas Arpagian
Rédacteur en chef de la revue *Prospective Stratégique*[1]

La cyber-guerre ou l'utilisation des technologies de l'information à des fins offensives représente assurément une forme très aboutie de conflit asymétrique. Puisque les parties prenantes y sont le plus souvent de nature différente : un particulier est en mesure de s'en prendre à une entreprise, un collectif militant peut conduire des attaques informationnelles ou informatiques contre un État, une société commerciale mener des opérations de dénigrement à l'encontre d'un concurrent… Et chacun est capable tour à tour de se faire passer pour ce qu'il n'est pas. Tels ces assauts numériques diligentés par un gouvernement mais officiellement revendiqués par des citoyens isolés. Bref, dans cette guerre des réseaux où les armes sont aussi bien les tuyaux qui véhiculent les données, que les informations ainsi diffusées, Internet fait désormais partie intégrante des arsenaux modernes.

On s'intéressera ici en priorité aux aspects informationnels de l'Internet, tels qu'ils peuvent être employés pour mener des opérations d'influence et de contestation, avec en retour des ripostes de la part des cibles visées, acteurs éco-

1. Nicolas Arpagian est également coordonnateur d'enseignements à l'Institut national des hautes études de la sécurité et de la justice (INHESJ), établissement public placé auprès du Premier ministre, et chargé de cours à l'IRIS et à l'Université Paris-Ouest (Paris X-Nanterre). Il est l'auteur de nombreux ouvrages, parmi lesquels : *La Cybersécurité*, Paris, coll. « Que Sais-je ? », Presses Universitaires de France, à paraître en septembre 2010 ; *L'État, la peur et le citoyen. Du sentiment d'insécurité à la marchandisation des risques*, Paris, Vuibert, 2010 ; *La Cyberguerre. La guerre numérique a commencé*, Paris, Vuibert, 2009 ; *Pour une stratégie globale de sécurité nationale*, avec E. Delbecque, Paris, Dalloz, 2008 ; *Liberté, égalité… sécurité*, Paris, Dalloz, 2007.

nomiques ou étatiques. On laissera donc délibérément de côté les opérations conduisant à surveiller, altérer, suspendre ou interrompre les systèmes de communication, soit l'aspect « tuyaux » évoqué précédemment.

Dans un univers numérique et dématérialisé, les règles du Droit de la guerre sont remises en question. Et des opérateurs privés, encore inconnus il y a une décennie, sont désormais des acteurs de dimension mondiale. C'est le cas de Google, Microsoft... Et plus récemment encore des réseaux sociaux.

Six années d'existence et plus de 400 millions d'utilisateurs à travers la planète. Ce sont en 2010 les deux chiffres qui caractérisent Facebook, le réseau social fondé par Mark Zuckerberg. Un phénomène « social » à part entière dès lors que le nombre d'inscrits a doublé au cours des douze derniers mois. Deux fois plus jeune – il fonctionne depuis trois ans seulement – son concurrent Twitter annonce déjà quelque 30 millions d'inscrits à sa plate-forme de *microblogging*. Un succès qui a incité les géants Google et Microsoft à mettre la main au portemonnaie pour indexer sur leurs moteurs de recherche respectifs les contenus des 8 milliards de ces très courts messages de 140 caractères au maximum, les *tweets,* actuellement en circulation sur les réseaux mondiaux. Face à cette multiplication exponentielle d'émetteurs de messages, et à cette masse croissante d'informations en circulation, il convient de s'interroger sur leur impact sur les opinions publiques, les entreprises et les gouvernements.

En observant les habitudes de consommation déjà acquises, on ne peut contester sa large diffusion auprès du grand public. En France, 77 % des internautes sont ainsi inscrits à un réseau social[1]. Toutefois, gare à certains décalages : en 2009, si 63 % de nos compatriotes connaissaient Twitter, ils n'étaient effectivement que 5 % à y participer.

Pays	**Temps passé par personne et par mois sur les principaux réseaux sociaux* en décembre 2009**
Australie	6 heures et 52 minutes
États-Unis	6 heures et 9 minutes
Royaume-Uni	6 heures et 7 minutes
Italie	6 heures
Espagne	5 heures et 30 minutes
Brésil	4 heures et 33 minutes
Allemagne	4 heures et 11 minutes
France	4 heures et 4 minutes
Suisse	3 heures et 54 minutes
Japon	2 heures et 50 minutes

** Facebook, Myspace, Twitter, Classmates et Linkedin.*
Source : Nielsen Company, janvier 2010.

1. Observatoire Ifop des réseaux sociaux 2009, www.ifop.com

Les réseaux sociaux, avec l'échange de données personnelles entre individus, remettent en cause le rôle d'intermédiaires des médias traditionnels, qui en sélectionnant, recoupant et d'une certaine manière filtrant les informations portées à la connaissance du public effectuaient un tri préalable des sujets traités. Bien évidemment, ces interventions n'ont jamais empêché des formes de manipulations variées. Mais celles-ci s'effectuaient avec une possible mise en cause *a posteriori* de la responsabilité du professionnel de l'information qui avait diffusé la nouvelle. Ainsi la 17e chambre correctionnelle du tribunal de Paris s'est faite une spécialité des délits de presse. Rien de tel dans les mondes numériques, où l'identité des émetteurs de messages diffamatoires est autrement plus difficile à découvrir que le nom d'un directeur de publication d'un journal diffusé en France…

Sans parler pour autant d'impunité numérique, il faut reconnaître que la souplesse d'utilisation de ces technologies, la modicité de leur prix, la rapidité d'intervention et la difficulté technique à remonter à la source de l'information font de ces outils des incontournables des opérations d'influence et de contestation. Mouvements politiques minoritaires, clients insatisfaits, militants isolés, opposants à des régimes autoritaires… tous vont peu à peu se saisir d'Internet et de ses déclinaisons pour faire entendre leur voix. Pendant longtemps, la conquête d'un territoire ou le renversement d'un pouvoir en place se caractérisait par la prise symbolique de la tour de la télévision et de la radio. Au XXIe siècle, c'est bien sur le réseau des réseaux que se conquièrent les avancées stratégiques. Et les cibles potentielles ne manquent pas. Ainsi, au printemps 2009 le cabinet Deloitte a interrogé un panel représentatif de cadres et de dirigeants d'entreprises états-uniennes pour son enquête *Social networking and reputational risk in the workplace*[1]. On y apprend que 74 % des employés interrogés estiment qu'il est facile de nuire à la réputation d'une société en utilisant les réseaux sociaux. Côté patrons, ils sont 60 % à considérer qu'ils ont le droit de savoir comment leurs collaborateurs les décrivent ainsi que leur entreprise sur lesdits réseaux sociaux. Pourtant, 27 % des salariés admettent ne pas prendre en compte les éventuelles conséquences de leurs messages ainsi diffusés sur la Toile. Ils sont même 37 % à avouer ne pas penser à la réaction de leur patron ou de leurs collègues, ni de leurs clients (34 %).

Les réseaux sociaux remettent en cause le rôle d'intermédiaires des médias traditionnels.

Ces chiffres – malgré la précaution indispensable à la lecture de tout sondage – doivent surtout faire prendre conscience qu'une part certaine des

1. www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_2009_ethics_workplace_survey_220509.pdf

commentaires et avis circulant sur le Net émanent bien de gens sincères et spontanés, et ne sont donc même pas le fruit d'une opération concertée de déstabilisation. Une précision importante à mentionner, quitte à contredire Andy Grove qui affirmait que « seuls les paranoïaques survivent ». Pourtant, il faut signaler que la très discrète Agence européenne en charge de la sécurité des réseaux et de l'information (ENISA) a choisi de consacrer en février 2010 un rapport intitulé « *Online as soon as it happens* »[1] aux menaces liées aux réseaux sociaux : pertes de données, intrusions dans la vie privée, disparition de la confidentialité des correspondances privées, atteintes à la réputation… sans parler des usurpations d'identité. Une démonstration symbolique intervint en 2008 quand un jeune Marocain eut l'idée de se faire passer sur Facebook pour Moulay Rachid, frère du roi Mohamed VI. Le phénomène « réseau social » est tel que l'assureur britannique Legal & General a commandité en août 2009 une enquête, *The digital criminal,* sur le comportement des internautes sur ces sites communautaires. Révélant ainsi que 13 % des inscrits à Facebook font accéder de parfaits inconnus au statut d'« amis », et que sur Twitter, ce chiffre grimpe à 92 %. Une fois ainsi référencées, ces personnes accèdent donc aux flux des messages. De quoi nourrir de manière très efficace des opérations de « social *engineering* » pour établir le profil personnel ou professionnel d'un individu. Et ensuite l'approcher plus aisément dans le monde réel puisque l'on connaît ses centres d'intérêts et son environnement social, et même ses déplacements, ce qui peut faciliter le cas échéant l'organisation de « visites » de son domicile en son absence.

De leur côté, les industriels ont bien saisi l'intérêt de miser sur l'effet réseau pour recommander leurs produits.

L'US Army avait intégré ce risque en interdisant à partir de l'été 2009 la connexion à ces sites communautaires à partir des ordinateurs branchés sur les réseaux militaires. Principales raisons invoquées : les possibles infections virales et la divulgation d'informations stratégiques sur le positionnement des troupes ou la composition des équipes envoyées sur les différents théâtres d'opération. Or, début mars 2010, David Wennergren, le secrétaire adjoint à la Défense en charge de la gestion de l'information et de la technologie a nuancé cette interdiction. En autorisant désormais l'accès à des sites tels Twitter, Youtube ou Facebook. Avec par contre de sévères restrictions en termes de types d'informations pouvant être diffusées sur ces canaux. D'ailleurs, l'état-major a d'ores et déjà annoncé que ces accès pourraient être suspendus ou limités si la sécurité des opérations militaires l'exigeait ou s'il fallait… préserver la bande passante. L'avantage que représente ce moyen d'entretenir une relation directe avec l'opinion publique semble donc ici compenser les menaces potentielles. Pour l'instant, en tout cas.

1. www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens

De leur côté, les industriels des années 2010 ont bien saisi l'intérêt de miser sur l'effet réseau pour recommander leurs produits ou services à une communauté de gens qui se connaissent, partagent les mêmes valeurs voire le même pouvoir d'achat. Par exemple, en 2009, la marque de lessive Cajoline est parvenue à rassembler 50 000 « fans » sur son profil *Facebook* tandis que le gel douche Axe en réunissait plus de 450 000. Une communication virale avec un rythme de diffusion inégalé. Le constructeur informatique Dell a ainsi estimé que les réseaux sociaux lui avaient permis de susciter 3,5 millions de « connexions sociales ». À chaque fois, l'entreprise dispose d'un lien direct avec ses acheteurs potentiels, qui ont fait spontanément la démarche de s'inscrire auprès d'elle : un vrai rêve de commerçant… Dell indique officiellement que les offres promotionnelles qu'il a diffusées sur Twitter ont généré quelque 6,5 millions de dollars de chiffres d'affaires, soit des performances qui font de ces canaux numériques à la fois des outils de promotion mais aussi de commercialisation. Les médias traditionnels ne peuvent guère rivaliser avec de tels retours sur investissement. Même si le phénomène va certainement se stabiliser au fur et à mesure qu'il atteindra une part majoritaire de la population, on comprend bien que les sociétés vont dans un avenir proche investir encore davantage ces territoires numériques.

Ce qui rend d'autant plus sensible la question du dénigrement et de la réputation numérique, et entraîne la nécessité impérieuse de protéger son capital de crédibilité et de confiance sur le Net. En avril 2009, la chaîne de restauration Domino's Pizza a ainsi dû contrer de toute urgence la mise en ligne sur plusieurs sites de partage de vidéos d'une séquence où l'un de ses employés maculait consciencieusement les plats livrés aux clients. Le PDG de l'enseigne a été contraint d'enregistrer sa propre séquence vidéo postée ensuite sur *YouTube* pour pallier cette situation de crise.

La crise qui a secoué le Kenya début 2008 a débuté par des échanges de SMS et des propos sur des blogs.

Mais les réseaux sociaux ne sont pas mis à contribution que dans la seule compétition commerciale. Ainsi, on se souvient que la crise qui a secoué le Kenya[1] au début de l'année 2008 a débuté par des échanges de SMS et des propos sur des blogs locaux qui ont donné le signal des violences. De même, lors des attentats qui ont frappé Bombay à la fin novembre 2008, le site Twitter a reçu près d'une centaine de messages toutes les cinq secondes émanant essentiellement de personnes se trouvant sur place avec leur téléphone portable. En Indonésie, en novembre 2009, 1 million d'internautes ont signé une pétition postée

1. « The brave new world of e-hatred », *The Economist*, 24 juillet 2008.

sur Facebook réclamant la libération des deux vice-présidents de la Commission pour l'éradication de la corruption (KPK). À ce propos, le chercheur en sciences sociales Jaleswari Pramodhawardani évoque même l'utilité d'un « Parlement en ligne »[1] pour compenser l'absence de communication entre les institutions de son pays et l'opinion publique.

Comme par réflexe naturel, sorte de réaction épidermique version numérique, la Toile a suscité elle-même ses propres contre-feux. A l'instar de l'application « Suicide Machine » mise en ligne en décembre 2009 qui propose aux internautes désireux de se retirer des différents sites sociaux d'automatiser l'effacement de leurs profils. Et ses initiateurs de mettre en avant le mérite d'un tel dispositif : alors qu'il faudrait passer plus de neuf heures et trente minutes pour supprimer manuellement un à un le millier d'« amis » d'un compte Facebook, ledit logiciel se propose de le faire seul en moins d'une heure. Avec la même frénésie déployée pour être présent sur le Net, on tente donc de s'en soustraire. Une méthode qui reste aux effets limités puisque les données soigneusement compilées par les moteurs de recherche restent largement disponibles. La notion d'effacement est donc toute théorique. Il convient davantage de miser sur un enfouissement des informations vous concernant dans les tréfonds des pages de réponse desdits moteurs de recherche, afin que vos données soient simplement moins accessibles. Des pratiques qui suscitent évidemment l'ire des réseaux sociaux. La guerre concernant ce patrimoine informationnel aura donc bien lieu. ■

1. Jaleswari Pramodhawardani, « Parlemen online », 6 novembre 2009, téléchargeable sur le site de Kompas (Jakarta): http://cetak.kompas.com/read/xml/2009/11/06/0342208/parlemen.online