POUVOIR NUMÉRIQUE ET PERTURBATION 2.0 : L'INTÉRÊT NATIONAL FACE AU DROIT À L'INFORMATION À L'ÈRE D'INTERNET

François-Bernard Huyghe

IRIS éditions | « Revue internationale et stratégique »

2017/1 N° 105 | pages 159 à 167

ISSN 1287-1672
DOI 10.3917/ris.105.0159

Pouvoir numérique et perturbation 2.0 : l'intérêt national face au droit à l'information à l'ère d'Internet

François-Bernard Huyghe
Directeur de recherche à l'IRIS.

« La nouvelle cyberguerre mondiale », titre un grand hebdomadaire français[1] au moment où ces lignes sont écrites, n'envisageant rien moins que l'arrêt complet d'Internet sous l'effet d'une attaque à distance. Le cyberespace n'est pas seulement un domaine de compétition économique et technologique plus ou moins pacifique entre nations, il devient également le lieu de toutes les craintes. L'espionnage par écrans interposés, le sabotage numérique à grande échelle, qu'ils soient menés par des États ou des organisations privées, éventuellement terroristes, suggèrent qu'il appartiendrait aux acteurs souverains de défendre aussi leurs « frontières » numériques. Des rapports de puissance et d'agression se dessinent. S'y ajoutent des scénarios inédits d'influence où des acteurs extérieurs tenteraient d'agir sur l'opinion d'un pays, en divulguant ses secrets, en sapant la confiance du public, en influant sur le résultat des élections ou sur des révoltes populaires. La défense de l'intérêt national passe désormais par la prise en compte de ces hypothèses, mais aussi par leur vérification de quelques fantasmes.

1. *Le Point*, n° 2316, 26 janvier 2017.

L'État : souveraineté et flux numériques

Contrairement aux prophéties des années 1990 sur la disparition des frontières ou la dilution de l'autorité au profit de réseaux autogérés, l'État est tout sauf impuissant dans le cyberespace. Des phénomènes tels que la « balkanisation du Web »[1], c'est-à-dire la capacité – relative – qu'ont certains acteurs souverains de conserver le contrôle des données et des échanges numériques sur leur territoire, les cyberconflits[2] ou l'espionnage planétaire « façon NSA » – relevant après tout d'une activité régalienne –, en attestent.

D'État à État, des rapports de contrôle et d'alliance inédits s'instaurent. Ils dépendent de la maîtrise par des acteurs souverains – ou par leurs grandes compagnies alliées à leur administration – de logiciels, de plates-formes et de réseaux, de la propriété intellectuelle et de la recherche, de la norme et de la localisation, du stockage et de la mise en corrélation des données, de la détermination des systèmes juridiques applicables. Il s'agit de rapports de puissance purs et simples.

Dans son action, l'État doit donc tenir compte des facteurs de domination technique, de sécurisation des données et des systèmes afin de réduire ses vulnérabilités. Le cyberespace est, certes, un domaine où « le code est la loi » et où la maîtrise des plates-formes, logiciels et données est déterminante. Pour autant, le politique n'est pas paralysé, ni la référence au territoire obsolète. Les acteurs souverains interviennent dans le cyberespace au nom d'un intérêt national, qui justifie tantôt des politiques industrielles ou de défense louables, tantôt les pires pratiques de censure – souvent au prétexte de mauvaises influences venues de l'extérieur – ou des cyberattaques d'espionnage, de déstabilisation, de pays à pays.

> Les acteurs souverains interviennent dans le cyberespace au nom d'un intérêt national

Le rapport « horizontal » d'État à État ou d'État à organisation extérieure se double d'un rapport « vertical », selon lequel l'État impose des normes à ses citoyens. Il leur alloue certains droits, comme celui au contrôle de leurs données personnelles ou des facultés d'expression en ligne, ou leur fournit certaines facilités comme la e-administration, c'est-à-dire lorsqu'un gouvernement fait relayer son autorité par des dispositifs en ligne. Il peut s'agir de contrôle, de censure, de persuasion exercé envers ses citoyens. En retour, ceux-ci peuvent affirmer leur autonomie, exercer une protestation, populariser une demande ou un soutien, lutter contre le pouvoir central, voire faire la révolution en utilisant

1. Cet article impliquant l'emploi de termes techniques, nous renvoyons le lecteur curieux de comprendre ce qu'est un « hack », l'« anonymisation » ou l'« inattribution », par exemple, au glossaire téléchargeable sur le site www.huygue.fr
2. Voir François-Bernard Huyghe, Olivier Kempf et Nicolas Mazzucchi, *Gagner les cyberconflits. Au-delà du technique*, Paris, Economica, 2014.

– mais pas exclusivement – des dispositifs numériques. Ainsi, la facilité de critique de l'information « officielle », la faculté de mise en contact et en commun, de coordination, l'incitation au passage à l'acte dans la « vie réelle » sur les réseaux sociaux confèrent du pouvoir politique à de nouveaux acteurs tout en retirant à d'autres. Cela participe d'une certaine décentralisation et confère un impact nouveau aux mouvements sociaux et activistes, au détriment donc de l'État.

La diagonale de la puissance

De plus en plus, le lien entre intérêt national et numérique passe par un rapport « diagonal », incluant les influences d'acteurs étrangers – États, organisations non gouvernementales (ONG), militants – sur les populations d'un pays. En la matière, il n'y a pas d'infinies façons de procéder : soit l'on peut soutenir des réseaux humains chez le voisin – un parti ami, par exemple –, soit l'on peut exercer un effet d'exemplarité par sa langue, sa technologie, sa culture, ses « valeurs » comme l'illustre le concept de *soft power*, soit encore l'on peut faire parvenir à la population ciblée des messages persuasifs et / ou lui donner accès à des médias – des moyens de communication, de réception ou d'émission – qui échappent aux autorités nationales. Ce dernier principe était déjà celui de la *public diplomacy* telle que la pratiquaient les États-Unis en créant des radios anticommunistes émettant au-delà du Rideau de fer (Voice of America, Radio Free Europe) dans les années 1960. C'est ce que font aujourd'hui, en sens inverse, des médias russes en ligne comme Russia Today et Sputnik. Mais si les fondamentaux sont les mêmes, le recours au numérique bouleverse tout un art d'exécution[1].

Deux innovations, d'ailleurs inséparables, déplacent les lignes de force et d'influence : la redistribution des capacités technologiques et la pénétration / publication des secrets des grandes organisations. L'intérêt d'un pays peut de plus en plus être affecté de l'extérieur et *via* la technologique numérique, négativement si l'on y voit une ingérence dans les affaires d'un gouvernement ou un encouragement à la violence, positivement si l'on pense qu'il s'agit de soutenir les dits démocrates ou de défendre une certaine conception de la vérité. La méthode passe par des « révélations » faites au public du pays-cible. Il peut s'agir de méthodes informatiques – pour se connecter, échapper à la police, pratiquer la cryptologie, anonymiser ses communications – ou de contenus numériques piratés ou « fuités » (plans secrets du gouvernement, archives compromettantes, documents inquiétants, etc.). L'arme du savoir – savoir technique et savoir de ce qui était caché – change ainsi les rapports entre les camps.

Dans le cas de formation ou fourniture de moyens, un État ou une organisation de type ONG peut offrir à une fraction de la population visée, à une

1. Voir François-Bernard Huyghe, *Désinformation. Les armes du faux*, Paris, Armand Colin, 2016.

opposition ou à une révolte des multiplicateurs technologiques de l'impact politique de ses actions. Ce que les Anglo-Saxons nomment l'*empowerment* du citoyen peut jouer dans divers sens. Le procédé n'est pas tout à fait nouveau. En 2010, à propos d'un conflit opposant Google et la Chine, qui imposait des restrictions sur les recherches menées sur son territoire, Hillary Clinton, dans un discours devant le Foreign Council, avait établi une sorte de doctrine : l'idée était de faire coïncider l'intérêt des États-Unis et l'expansion d'un Internet libre et non censuré, de fournir une aide de l'administration aux cyberdissidences sous forme de technologies et de conseils, de refuser de laisser des entreprises américaines coopérer avec des systèmes de surveillance du Web par des gouvernements autocratiques[1].

Lors des « printemps arabes », les révoltes en ligne furent aidées depuis l'Occident de deux façons. D'une part à travers un discours médiatique enthousiaste exaltant les « Twitter Revolutions », aussi appelées « révolutions 2.0 », et encourageant les opposants à communiquer en ligne sur leur cause et à incarner le slogan « nous sommes les médias » – et même si le rôle de médias « traditionnels » comme Al-Jazira et celui de réseaux militants créés avant 2011 a été tout sauf négligeable. D'autre part, ce soutien s'est aussi manifesté de façon plus technique : celui de grandes compagnies, Google en tête, prenant nettement partie et aidant les communications, d'ONG, telle la Albert Einstein Foundation, formant aux techniques de l'activisme en ligne, ou encore de groupes comme Anonymous ou Lulzsec offrant aux forces d'opposition des algorithmes de connexion, d'anonymisation mais aussi des moyens pour attaquer les sites gouvernementaux[2].

> Il ne suffit pas de distribuer des logiciels ou de fournir des connexions pour renverser tous les régimes autoritaires

Quelques années plus tard, il faut admettre plusieurs conclusions. Premièrement, il ne suffit pas de distribuer des logiciels ou de fournir des connexions pour renverser tous les régimes autoritaires, qui peuvent d'ailleurs fort bien s'adapter à la lutte d'influence dans le cyberespace. Deuxièmement, ce qui sert à protéger de sympathiques protestataires peut servir, *in fine*, à des gens plus redoutables. L'on a notamment découvert la capacité de recrutement, de propagande, de coordination, de formation de communautés djihadistes de l'État islamique. D'où les tentatives récentes des pays occidentaux de mieux contrôler la parole sur Internet, de surveiller les réseaux sociaux, de supprimer des sites et des comptes, de coopérer avec les géants de l'Internet – Google, Apple, Facebook, Amazon, communément regroupés sous l'acronyme GAFA – dans le but de faire disparaître les « discours de haine », d'empêcher l'accès aux contenus incitatifs[3],

1. The prepared text of U.S. of Secretary of State Hillary Rodham Clinton's speech, delivered at the Newseum in Washington, DC, 20 janvier 2010
2. Voir le dossier « Réseaux : après l'utopie », *Médium*, n° 29, octobre-novembre-décembre 2011.
3. Ainsi de Jigsaw de Google, dispositif censé envoyer vers des contenus sains ceux qui feraient des recherches indiquant un intérêt pour les thèmes djihadistes.

d'utiliser les *big data* pour repérer l'adversaire, etc. Face à cela, les partisans du califat recourent, dans leur lutte asymétrique, à toujours plus de sophistication technologique, en utilisant par exemple des messageries sécurisées comme Telegram, et dispensent à leurs partisans des conseils fort pédagogiques. Les revues de Daech en ligne donnent ainsi des cours de cryptologie, d'utilisation du « Dark Web », de désactivation de la géolocalisation, d'utilisation de téléphones portables sécurisés. Autant d'éléments qui n'ont rien à envier à la formation dispensée, en d'autres temps, aux cyberdissidents ou aux journalistes menacés dans des pays autoritaires.

L'intérêt national au défi de la « guerre » de la transparence

L'actualité vient aussi démontrer l'impact, direct et indirect, d'une autre stratégie : celle de la révélation publique de secrets numériques[1]. À partir du moment où la plupart des activités des individus et *a fortiori* des organisations publiques ou privées sont enregistrées numériquement, le risque est que les données soient interceptées ou recopiées sur un quelconque point de passage ou de stockage, d'où une perpétuelle possibilité de fuite. La fuite peut alors résulter d'une décision humaine. À l'instar de Bradley Manning ou d'Edward Snowden, il peut s'agir de quelqu'un qui, par exemple, a prêté serment de garder confidentiels des documents, mais qui finit par éprouver un scrupule moral et communique alors ce secret – malversation, atteinte aux droits de l'homme, bavure militaire, système de surveillance, etc. – qui lui paraît désormais honteux. Au nom d'une valeur supérieure, comme le bien commun ou la justice, il accepte de passer pour un traître, courant le risque d'extraire des informations, et surtout de les mettre sur la place publique, ce qui le fera forcément soupçonner. La démarche diffère de celle de l'espion, qui travaille par idéologie, par ordre, par appât du gain, mais, en principe, en faisant tout pour éviter que l'organisation espionnée ne se sache pénétrée. Il existe une autre possibilité, qui peut d'ailleurs se combiner avec la première : des pirates informatiques pénètrent à distance dans un système ou un appareil, y prélèvent des données qui devraient être protégées et les divulguent. Là aussi, il y a une différence avec une attaque d'espionnage informatique pur, qui chercherait à ne pas être décelée, ne serait-ce que pour garder le plus longtemps possible un accès à des ressources précieuses.

Ces deux cas renvoient à une certaine compromission, que ce soit au sens informatique – attenter à la fiabilité d'un système de protection numérique –, ou de réputation et d'image d'un individu ou d'une organisation, le tout aboutissant à une forme de scandale. En outre, si les documents révélés peuvent

1. Voir le dossier « Secrets à l'ère numérique », *Médium*, n° 37-38, octobre 2013-mars 2014.

être truqués, une campagne de communication peut également tenter de les faire passer comme tels. Les fuites provoquées par des lanceurs d'alerte, les piratages informatiques et les faux avérés ou supposés, ce que les Anglo-Saxons appelleraient de façon plus sonore des *leaks*, des *hacks* et des *fakes*, modifient encore la donne de l'intérêt national face à la transparence. Et l'apparition d'organisations militantes ou non gouvernementales qui se vouent à l'avènement de la transparence constitue un autre facteur interférant dans cette « guerre ». La plus connue est Wikileaks, apparue en 2006, rendue célèbre par son fondateur charismatique, Julian Assange, et imitée depuis par d'autres. Le principe énoncé par J. Assange lui-même est clair : persuadé que les gouvernants tendent à détourner le pouvoir à leur profit et que tout cela produit mécaniquement une bureaucratie numérique en charge des manipulations de l'opinion, il affirme que le peuple pourra, en quelque sorte, reprendre le pouvoir confisqué, pourvu que ceux qui ont la compétence technique – l'art du piratage informatique en particulier – lui dévoilent les arcanes et manœuvres des puissants. Wikileaks, dont le principe est de ne publier que des documents authentiques, embarrassants pour les « fuités », et au risque de contrevenir à leurs lois, se réclame donc de droits supérieurs, ceux des citoyens à qui l'on cache ce que l'on fait en leur nom[1].

S'en suit, dans un premier temps, ce qui ressemble à une simple logique d'action / réaction : les lanceurs d'alerte publient l'information, relayée souvent par de grands journaux nationaux, provoquant l'indignation de l'opinion. Puis, les autorités réagissent, souvent en dénonçant les conséquences abominables pour la sécurité nationale et en réprimant les lanceurs d'alerte. Ainsi, lorsque le soldat Manning transmet, en 2010, divers documents militaires à Wikileaks, dont la fameuse vidéo d'une bavure en Irak qui coûta la vie à des journalistes, le gouvernement américain explique que ces fuites mettent en danger la vie de soldats ou d'agents de terrain. B. Manning est condamné à trente-cinq ans de prison et Wikileaks subit divers désagréments, comme le blocage de ses comptes de paiement. En un sens, ce mécanisme n'est pas sans rappeler – dimension numérique mise à part – l'affaire Ellsberg : analyste à la Rand Corporation, Daniel Ellsberg révéla, en 1971, *via* le *New York Times*, 7 000 pages de documents – papier à l'époque – sur la politique secrète des États-Unis au Viêtnam et fut poursuivi pour vol et espionnage. La procédure fut finalement abandonnée et D. Ellsberg recouvra sa liberté sous la présidence Nixon. Le débat éthique se posait alors en termes assez simples : droit de savoir des gouvernés *versus* normes d'État et sécurité nationale.

Les fuites provoquées par des lanceurs d'alerte, les piratages informatiques et les faux avérés ou supposés modifient encore la donne de l'intérêt national

1. Voir Geoffroy de Lagasnerie, *L'art de la révolte. Snowden, Assange, Manning*, Paris, Fayard, 2015 ; et Florence Hartmann, *Lanceurs d'alerte. Les mauvaises consciences de nos démocraties*, Paris, Don Quichotte, 2014.

La lutte des révélations dans le cadre de la démocratie et des intérêts nationaux : le cas de l'élection présidentielle américaine de 2016

Or, voici que des événements récents révèlent comment l'art de la fuite et de la contre-fuite – réfuter, discréditer la source, en dénoncer les intentions suspectes, etc. – peut à la fois déclencher des crises politiques, pour ne pas dire des conflits, et inspirer des stratégies de plus en plus sophistiquées et imbriquées. À titre d'exemple, l'affaire des courriels du Parti démocrate livrés au public à l'occasion de l'élection présidentielle américaine de 2016 s'est inscrite dans un contexte où :

– la candidate Hillary Clinton avait déjà été compromise par la révélation de ses courriels privés, mais dans le cadre de deux enquêtes du Federal Bureau of Investigation (FBI), et nullement par un acte de piraterie informatique ;

– la tension était à son comble entre l'administration Obama et la Russie : les accusations de cyberpiraterie fusent contre Moscou, mais aussi les menaces de rétorsion par des moyens informatiques – contre-attaque contre des systèmes informatiques russes par exemple – ou non ;

> L'art de la fuite et de la contre-fuite peut déclencher des crises politiques, pour ne pas dire des conflits

– Julian Assange, réfugié à l'ambassade d'Équateur à Londres depuis trois ans, n'a alors évidemment aucune raison de ménager l'administration et la candidate démocrates ;

– l'affrontement électoral entre Hillary Clinton et Donald Trump finit par se muer quasiment en une lutte entre médias « classiques » – journaux et télévisions – favorables à la première ou du moins plus désireux de révéler des scandales, notamment sexuels, sur D. Trump que sur H. Clinton et, d'autre part, le monde des médias sociaux supposés plus prompts à dénoncer les mensonges des élites et de la candidate démocrate.

Dans ce contexte de tensions, sont divulguées, et bruyamment applaudies par D. Trump, deux séries de documents arrachés au Parti démocrate et au directeur de campagne d'Hillary Clinton. Apparemment piégés par des pirates informatiques – *hack*, et non *leak* –, dont au moins une fois avec une naïveté désarmante, en acceptant de donner un mot de passe en réponse à un mail trompeur, les démocrates voient ainsi être mis sur la place publique, *via* Wikileaks, des courriels, qui seraient donc des documents authentiques. Ceux-ci témoignent des manœuvres au sein du parti pour favoriser la candidate, de la connivence entre cette dernière et certains journalistes, des rapports financiers pour le moins ambigus avec des lobbyistes et de grandes sociétés *via* la Fondation

Clinton, etc. Somme toute, cela s'apparente au matériel que pourrait produire du journalisme d'investigation ; il est ici prélevé illégalement et sans doute à distance.

Dans l'interrègne entre l'élection de D. Trump et le départ effectif de Barack Obama, l'affaire quitte le terrain des révélations politiques – la question de la source et de ses intentions faisant d'une certaine façon oublier la question du contenu des mails ainsi que celle de leur authenticité – pour passer sur le plan géopolitique et idéologique. Sur la base d'un rapport de la Central Intelligence Agency (CIA), non endossé par l'ensemble des agences de renseignement américaines toutefois, l'administration Obama et les médias favorables à la candidate démocrate, c'est-à-dire la majorité d'entre eux, stigmatisent une interférence russe. L'idée est que des pirates soutenus ou dirigés par Vladimir Poutine, et par l'intermédiaire de son complice J. Assange, auraient délibérément favorisé l'élection de D. Trump[1]. La conspiration « Russes, plus lanceurs d'alerte, plus populistes » ainsi présumée, les médias de type *Washington Post* ou NBC soutiennent la thèse d'un « vol » de l'élection par un candidat tricheur, qui serait la marionnette d'une puissance étrangère. La double atteinte à la démocratie et aux intérêts nationaux établie, le président B. Obama, en exercice jusqu'au 20 janvier 2016, menace la Russie de rétorsion contre ce qu'il assimile à une agression et à une forme d'ingérence. Ce qui, suivant la doctrine cyber établie sous le même président, pourrait justifier une rétorsion par des armes informatiques ou non informatiques. Pendant ce temps, certains parlent d'aller jusqu'à annuler l'élection de D. Trump, marionnette des Russes.

S'ouvre évidemment une violente controverse politique interne. Certains remettent en cause les accusations de la CIA[2] – organisation qui, après tout, avait bien « découvert » des armes de destruction massive en Irak et proféré d'autres contre-vérités, et était intervenue dans quelques élections de pays étrangers –, voire le processus même, quelque peu maccarthyste ou complotiste, consistant à tout expliquer par l'action des « agents de l'étranger ». L'inattribution des cyberattaques étant la règle dans le cyberespace, il est probable que l'on ne puisse jamais établir avec certitude si les fuites, ou seulement l'une d'entre elles, ont été commanditées par la Russie, réalisées par des groupes de pirates informatiques établis sur son territoire – et peut-être tolérés par le Kremlin –, et que l'on ne sache jamais qui s'était concerté avec qui ou a commandé quoi.

Reste l'essentiel : les fuites pourraient à la fois devenir de plus en plus fréquentes, à la fois pour des raisons techniques, mais aussi « sociologiques », en raison de la popularité des lanceurs d'alerte. De fait, elles pourraient avoir des conséquences plus graves, non pas tant au premier degré par l'indignation populaire qu'elles provoquent *via* les médias, mais comme facteur de

1. Eric Lipton, David E. Sanger et Scott Shane, « The Perfect Weapon: How Russian Cyberpower Invaded the U.S. », *The New York Times*, 13 décembre 2016.
2. Glenn Greenwald, « Anonymous Leaks to the Washpost About the CIA's Russia Beliefs Are No Subsitute for Evidence », *The Intercept*, 10 décembre 2016.

déstabilisation du jeu politique. On verrait ainsi s'opposer, selon diverses configurations, un camp de « révélateurs », cherchant, au nom de la transparence, à déstabiliser la partie adverse par la mise à jour de ses turpitudes – véritables ou imaginaires –, face à un camp de « dénonciateurs » se posant en défenseurs de la démocratie. La rhétorique de ces derniers stigmatiserait les agents secrets, les faussaires, les complotistes et les populistes qui délireraient sur les réseaux sociaux. Singulière fracture idéologique autour de l'établissement de la réalité, ce n'est finalement pas par hasard que le mot « post-vérité » (« post-truth ») a été choisi comme mot de l'année par l'*Oxford Dictionary*[1]. ■

1. « L'ère du "post-factuel" et de la "post-vérité" en politique », *Le Nouvel Économiste*, 26 septembre 2016.