



Revue internationale
International Web Journal
www.sens-public.org

Source et fuites : du sens des flux de données numériques

YANNICK MAIGNIEN

Source et fuites : du sens des flux de données numériques¹

Yannick Maignien

« Je suis militant, journaliste, programmeur de logiciels, expert en cryptographie, spécialisé dans les systèmes conçus pour protéger les défenseurs des droits de l'homme ». Julian Assange

« Dans les églises byzantines, le sanctuaire est clos par l'iconostase. Dans une société athée, par le secret d'État ». Régis Debray, *Loués soient nos seigneurs. Une éducation politique*. p. 585. Cité en exergue de « *Secrets d'États* » d'Olivier Forcade et Sébastien Laurent, Armand Colin, 2005

« Il n'y a pas de secret d'État, c'est pas possible. L'information est immédiatement disponible », Nicolas Sarkozy. Conférence Etalab E-G8 6 décembre 2011

Politique et numérique, entre secret et transparence

Depuis Machiavel, pour le moins, la question de la dialectique du secret et de la transparence, du privé et du public, de l'opacité et de la liberté, est devenue de plus en plus prenante du discours et de la théorie politique. L'histoire récente a porté cette question à de hauts degrés de sophistication, avec une institutionnalisation du secret d'État, une judiciarisation des règles d'accès, de l'information administrative et des pratiques de divulgation militaire, policière ou politique – c'est-à-dire de renseignement –, de plus en plus techniques et élaborées.

Cependant le numérique et Internet viennent de montrer ces dernières années qu'il fallait sans doute repenser cette relation en fonction de capacités quantitatives et qualitatives de réplication, donc de duplication et de publication, sans commune mesure avec celles liées aux documents analogiques, dans leur origine comme source, comme dans leur diffusion publique.

La fiabilité des sources d'information et la manipulation de celles-ci – la gestion des fuites – existent depuis au moins aussi longtemps que la presse ou d'autres médiations messagères interviennent dans la gestion du secret et des nécessaires formes de divulgation publique. Mais la

¹ Communication donnée le 13 avril 2012 au colloque « Copie, mode d'emploi », organisé à la Fondation des Treilles par Louise Merzeau et Régis Debray de la revue *Médium*.

dynamique du numérique impose maintenant la transitivité du verbe au lieu du substantif : on dit maintenant *fuite*, *sourcer*. Comme si la dynamique même de ces verbes semblait interdire d'en arrêter un sens distinct, d'en séparer l'interaction.

Le numérique et Internet ont modifié profondément le régime et le statut d'autorisation d'accès à l'information en approfondissant les formes de secret et de divulgation. C'est ce sur quoi je voudrais m'interroger à partir de l'événement créé par Wikileaks et Anonymous, surtout depuis 2010.

En quoi cette capacité illimitée de copie, de réplique, de dissémination spatio-temporelle généralisée du numérique change-t-elle les conditions du secret, de la nature des sources et de leur protection, de l'anonymat ?

En quoi la rapidité quasi instantanée et mondialisée de diffusion d'un quantum d'information numérique sans égal semble échapper à toute maîtrise ? – la fuite ayant très vite des dimensions catastrophiques, à la hauteur de l'ampleur du gisement ou de la ressource captés, un peu comme dans les problèmes de fuite de plate-forme pétrolière, gazière ou nucléaire. Plus on fore profond, plus les circuits de canalisation sont complexes, et plus la fuite est risquée. La fuite s'est considérablement socialisée, mondialisée. L'échelle de la fuite est également à la mesure de la « neutralité du Web », de l'ouverture de son protocole et de la publicité de ses normes imposant un a priori de transparence.

WIKILEAKS : le secret d'État face au numérique

Au fond, et historiquement à la suite de nombreux conflits contemporains, le numérique et Internet ouvrent potentiellement à de nouvelles formes de liberté publique, informationnelle et communicationnelle. Mais politiquement, quelle forme de secret d'État, au sens de la puissance publique, sommes-nous prêts à accepter pour en organiser l'épanouissement ?

C'est ce nouveau « grand écart » entre transparence et secret, clés de nouvelles stratégies possibles, qu'il faut souligner à travers les exemples de Wikileaks et d'autres sites Web équivalents. Plus l'information publique est ou semble transparente et plus le secret s'approfondit avec des formes renouvelées d'opacité.

On le sait, Wikileaks et son fondateur Assange se sont fait connaître d'abord par la communication d'un rapport sur la corruption d'État au Kenya, à la suite de la présidence Harap Moy, mais surtout par la diffusion d'une vidéo de l'armée américaine en Irak montrant comment un hélicoptère Apache mitraille froidement deux journalistes de Reuter et des civils irakiens. Images montées pour plus d'impacts et présentées lors d'une conférence de presse. Wikileaks c'est aussi la divulgation sur Internet de l'ensemble des comptes de la Banque Bär, banque camouflant des circuits de blanchiment et de paradis fiscaux. C'est également la divulgation, en

liaison avec les activités de hacking d'Anonymous, de documents de l'Église de scientologie. C'est surtout la divulgation de plus de 250 000 *cables*, télégrammes diplomatiques américains, publiés par le truchement de la presse internationale, associée à cette diffusion publique, pour des raisons de liberté d'information et d'impact éditorial.

Le mode opératoire de Wikileaks est au croisement de cet impératif de protection des sources et de maximisation de l'impact public.

Protection des sources. Comme Anonymous, Assange a compris que dans le monde contemporain et la complexité de ses institutions et entreprises, une grande partie des « agents » employés ne partagent pas nécessairement les vues des institutions auxquelles ils appartiennent. Devant cette « crise de conscience » ils peuvent être amenés à dénoncer les raisons de ces désaccords, mais sont dans l'incapacité de le faire par peur de rétorsion. Il faut donc que la protection de l'anonymat le plus complet leur soit assurée. Cette « mission » de « Whistle blower », de lanceur d'alerte, est reconnue et valorisée dans certaines cultures, juridiction ou institutions. Elle est condamnée dans d'autres.

Techniquement, il faut donc que le « lanceur d'alerte » puisse déposer ses informations sans être identifié, localisé ou repéré, dans une sorte de « boîte au lettre morte ». Le déposant doit pouvoir copier des masses énormes de fichiers et les verser dans cette boîte en toute sécurité. Ce dispositif crypté doit être inviolable, et il semble que jusqu'à maintenant cette confiance n'ait pas été trahie et que techniquement, le dispositif de cryptage et de fragmentation des copies assuré par l'équipe d'Assange soit solide. Inversement, Wikileaks doit offrir la lecture au maximum de copies de ces contenus, notamment à la presse, afin de maximiser l'impact. De ce point de vue, Wikileaks se considère comme « propriétaire » et éditeurs de ces données, afin de capitaliser sur son rôle « d'organisateur collaboratif de fuites ». En même temps, et pour des raisons symétriques de sécurité informatique, Wikileaks est organisé en réseau de serveurs à l'échelle mondiale, afin de copier en autant de sites miroirs les données recelées, ce surtout à partir du moment où des menaces étatiques de rétorsions juridiques, financières ou techniques veulent empêcher le fonctionnement de la plate-forme.

C'est donc ce dispositif technique sur le Web qui est au cœur de cette nouvelle relation entre secret et transparence à l'ère numérique.

Julian Assange

Julian Assange est l'incarnation visible de l'ensemble du projet Wikileaks. Assange, y compris dans le moindre détail biographique, est symptomatique, paradigmatique d'une version post-moderne de cette relation politique au secret.

L'individu Assange, son origine australienne, sa biographie familiale complexe, son profil de hacker, sa formation autodidacte, sa tenue vestimentaire, comme sa capacité à s'abstraire pour travailler des dizaines d'heure de suite, son investissement libertaire, sa vie sexuelle et les aléas de ses relations, ses déboires juridiques privés mêlés (ou non) aux problèmes politique du *cablegate*, etc., autant d'éléments d'une saga représentative d'une nouvelle figure du secret autant que d'une nouvelle forme de la publicité, au sens politique du terme. Assange, par cette clandestinité itinérante « semble s'inscrire dans l'hétéronomie supposée de l'homme moderne, sans moi unifié en raison de la multiplicité des groupes auxquels il s'apparente² ». Au sens propre d'une « légende », entretenue notamment par les récits de son ancien ami, Daniel Domscheid-Berg³, Assange semble insaisissable, à tous points de vue. Complexe également la personnalité de Bradley Manning, la source présumée, condamnée par les États Unis à 52 ans d'incarcération, comme auteur supposé des fuites militaires, le traître, lui-même trahi par son ami Lamo... Manning qui aurait recopié les milliers de câbles sur un CD de Lady Gaga... Tous les ingrédients d'une fable cybernétique. Comme le dit Dewerpe à propos de l'espion :

« Révélée dans l'expérience clandestine de la personnalité dédoublée, la gestion du secret personnel que met en œuvre l'espion de notre époque correspond à une économie particulière du sujet qui organise, à un point extrême du dispositif des comportements psychologiquement possibles et socialement réalisés, la tension entre l'espace du secret et celui de la publicité et éclaire ainsi l'étape contemporaine de l'histoire sociale de l'identité personnelle⁴ ».

Fuites et enjeux de l'ouverture d'Internet

Il a souvent été souligné combien Internet dans ses origines comme dans sa gestion était lié à une double culture et contre-culture américaine de liberté absolue d'information, la cybernétique. Liberté d'information garantie par le Premier amendement de la Constitution américaine. Idéologie qu'on retrouve par exemple dans Wikipedia et qui sert de référence pour les plus grands *trusts* privés du numérique. Internet est devenu un monde en soi, avec de nouvelles règles d'ouverture (*open*, ouvert, transparent, sinon *free*, à la fois libre et gratuit).

De fait, cette transparence est directement issue des Lumières (comme opposée au secret de l'obscurantisme, c'est-à-dire de l'Absolutisme) :

² Dewerpe, Alain, *Espion, une anthropologie historique du secret d'État contemporain*, Paris, Gallimard NRF, 1994, p. 311.

³ Domscheid-Berg, *Inside Wikileaks*, Paris, Grasset, 2011.

⁴ Dewerpe, *op. cit.*, p. 314.

« En affirmant le principe de publicité, l'opinion publique abolit la dissimulation et le secret : elle convoque la transparence, la franchise, le discours explicite et vrai que la raison exige. »⁵

Avec la transparence libérale, l'affirmation du règne de la Loi et de la légitimation du pouvoir par une volonté générale fondatrice de la souveraineté ouvre à une nouvelle délimitation de la frontière entre le secret et le public. Cet impératif de transparence, lié à la neutralité du réseau, s'étend progressivement à tous les secteurs d'édition, des médias, de l'administration, puis surtout avec les réseaux sociaux, à toute la société. De façon licite, ou dénoncé comme illicite par de nombreux acteurs privés, les contrecultures s'emparent de cette dialectique parce que très vite les tentatives de limiter les possibilités numériques d'expression du Net, (sous couvert de « protéger le droit », par exemple les récentes initiatives contre la *piracy*, SOPA, ACTA⁶, Hadopi, etc.) sont combattues elles mêmes par des tentatives de hacking. Sans rentrer dans le détail de cette problématique de la transparence, il faut souligner l'ambivalence complexe, non fixée, du licite et de l'illicite, à partir des potentialités de ce média viral, mémétique qu'on retrouve dans Facebook et les réseaux sociaux. Le pouvoir de libération du Net est loué dans les révolutions arabes, en même temps qu'Internet sert à tracer les opposants (DRM). On a vu Hillary Clinton soutenir aussi fortement ce pouvoir de libération de l'Internet que, quelque temps après, les poursuites contre Wikileaks.

Ce qui nous intéresse ici, c'est le pouvoir de fuite, de divulgation et de dévoilement dont est capable le réseau numérique. Comme le dit Assange, à la tête de quelques dizaines de personnes, on peut « provoquer de très grandes réformes politiques avec une très faible consommation d'énergie ». La fuite est une faille minuscule dans le circuit, suffisante pour la sortie massive de données. Wikileaks s'inscrit dans cette puissance de diffusion, de révélation, sans aucune mesure avec la puissance des dictatures ou des monopoles détenteur de secrets ou de conspiration.

L'économie des fuites, bien gérée, est d'une productivité prodigieuse : rumeur, dissémination des données, images choc, distribution planétaire des données, tout informe sur tout, à partir du Web et au sein du cyberspace.

On le sait, le *cablegate* a soulevé un débat assez irréal sur la crainte de la « dictature de la transparence⁷ », totalitaire, notamment dans le domaine diplomatique. D'une part, il s'est révélé que les *cables*, aussi déplaisants qu'ils soient pour montrer le cynisme et l'arrogance de la Diplomatie américaine, ne révélaient peut-être pas autre chose que ce dont on se doutait. Par

⁵ Dewerpe, op. cit., p. 77.

⁶ *Stop Online Piracy Act, Anti-Counterfeiting Trade Agreement.*

⁷ Elisabeth Roudinesco, « Wikileaks : la dictature de la transparence », *Libération*, 2 décembre 2010
<http://www.liberation.fr/monde/01012305697-wikileaks-la-dictature-de-la-transparence>

ailleurs, la diplomatie officielle de représentation n'est de fait, et historiquement, pas équivalente aux services de renseignement. Pour l'essentiel, le débat s'est caractérisé par une hypocrisie assez mesquine de la part de détenteur de petits secrets.

Wikileaks et les médias

Wikileaks a dû par ailleurs prouver sa fiabilité dans la maîtrise du dispositif aux yeux des médias. Il lui a fallu faire preuve d'une crédibilité, d'une autorité, pour authentifier les sources et donc donner d'autant plus d'impact aux fuites. Dans cet exercice, Assange avait absolument besoin du secours des grands médias. C'est le cas des titres de la Presse écrite qui ont contractualisé avec lui, *The Guardian*, *El Pais*, *Der Spiegel*, *Le Monde*, *New York Times*.

Le besoin des journaux pour traiter l'info des 250 000 câbles était évident pour filtrer, hiérarchiser et synthétiser les *cables* intéressants. Mais c'est surtout la capacité de divulgation, de publication et de valorisation éditoriale qui a permis de maximiser l'impact des données livrées à et par Wikileaks.

Finalement, la question de savoir si Wikileaks est un média – plutôt qu'un organe d'espionnage (il n'est pas à la source des informations) – ou une sorte d'infra ou de méta média (intermédiaire entre sources et médias) est une bonne question. On comprend qu'Assange ait particulièrement soigné cette relation, sachant que sa notoriété médiatique est aussi sa ligne de défense.

L'ouverture des données publiques

Une des formes actuelles de la transparence numérique se développe à partir de l'Open data et des possibilités de traitements des données par le Web sémantique : faire produire du sens inédit à partir de données décontextualisées. L'ouverture des données publiques est l'un des prolongements de l'Open data, et le débat sur la confidentialité, l'anonymisation ou la ré-utilisation des données administratives, est des plus important.

Il ne s'agit néanmoins pas de données « sensibles », et la ré-organisation du secret administratif, ou du moins du domaine réservé, sera intéressant à apprécier.

On reproche à Google de vouloir faire, à partir de ses différents services, ce que l'on pousse au contraire à faire avec l'ouverture des données publiques ! Dans l'état actuel des choses, la réglementation européenne sur l'impossibilité de composer des données est encore peu cohérente avec le mouvement de l'Open Data, comme le montre le projet Data Connexion sur les applications et la ré-utilisation des données ouvertes.

L'État organise lui-même la transparence des données publiques, mais il y a encore loin entre cette volonté d'ouverture et la réalité des domaines réservés.

« Si on fait fuiter une étude, l'administration nous identifie immédiatement. Avec les suppressions de postes, on se retrouve de plus en plus souvent seul en charge d'une enquête. Il est donc très facile de nous repérer. On risque gros, j'ai des collègues qui sont en procédure de radiation. »⁸

On assiste donc à la fois à la possibilité du croisement des données publiques comme valorisation capitalistique, alors même que le croisement des fichiers sensibles fait l'objet d'une surveillance et d'un contrôle absolu, ou d'une exploitation par des firmes du renseignement (DPI *Deep packet inspection*, Inspection profonde de paquets). Il n'est pas certain que les frontières entre les modalités de transparence de l'une et de l'autre de ces possibilités d'exploitation des données soient aussi nettes et étanches que cela.

Open data et Web sémantique

L'ambivalence d'un Web plus secret et plus dévoilé en même temps est en marche. Le Web sémantique, par l'expression logique des données, autonomise à l'infini les combinaisons graphiques de construction. Le Web deviendrait plus un gisement de données qu'une collection de documents d'information. Les possibilités de croisement des données, de construction d'ontologies donnant ex post du sens aux data, renforcera les capacité de calcul, d'inférence et de simulation, à partir des données. Qui disposera de ce pouvoir disposera du secret. Là encore, plus l'ouverture de données sera effective, plus sera puissante la maîtrise des graphes que sauront construire de nouvelles puissances informatiques, que ce soit sur les données personnelles, nominales, vitales, sociales ou locales, bref sur tous ces matériaux du monde réel qu'exploite et code le cyberspace.

Même pour les données les plus secrètes, leur traitement doit être fluide, sans obstacle. Car, pour être efficace, le traitement des données exige accès et partage : il ne peut être ralenti par des procédures administratives trop lourdes, une multiplication de paliers de sécurité ou un cloisonnement rigide.

« Il faut se rappeler que l'incapacité des agences américaines de renseignement à relier entre elles des informations recueillies par différentes administrations avait été vertement critiquée par la Commission nationale sur les attentats du 11 septembre 2001 ».

Felix Stadler. C'est cette fluidité qui pourrait être attendue du Web sémantique.

⁸ *Libération*, 5 avril 2012, « Les statistiques de l'Éducation nationale sont-elles un secret d'État ? »

<http://www.liberation.fr/societe/01012400660-les-statistiques-de-l-education-nationale-sont-elles-un-secret-d-etat>

Notons également que la croissance du ratio entre *Humint* (*Human Intelligence*) et *Sigint* (*Signal Intelligence*), dans les investissements des agences, au détriment du *Humint*, est en voie d'exploser, et devrait être repensé si le renseignement veut vraiment maîtriser cette révolution du Web sémantique.

Sources, secrets et pouvoirs numériques

La source est en rapport avec le caché absolu. C'est l'« Origine du monde ». Mais c'est aussi Courbet repris par Duchamp dans « Étant donnés : 1° la chute d'eau, 2° le gaz d'éclairage... », le trou dans la porte de l'icônostase de l'intime, mais aussi montage et illusion. Encore des fluides.

Même pour les plus grands fleuves, le Nil, la source est parfois non-identifiée, difficile d'accès, mythique.

En même temps, la source n'a de sens que par le fleuve qui la manifeste. Si un secret reste discret, il n'a pas vraiment de valeur. Original sans copie, la copie infinie par la fuite, le voyeur, révèle l'illusion. La source est secrète, sacrée, protégée, la porte de l'icônostase est close, mais les icônes doivent circuler.

C'est par sa potentialité de connaissance, sa puissance de diffusion, sa maximisation d'impact qu'une information « secrète » devient dangereuse, prend sens politique.

En corollaire, le secret ne disparaît pas avec la transparence numérique, au contraire. D'après le *Washington Post*, le nombre de documents classés « secrets » aux États-Unis a explosé entre 1996 et 2009, passant de 5,6 millions à... 54,6 millions.

Il faut ici rappeler que le code numérique en informatique est historiquement et directement issu de la même matrice que l'algorithme de cryptage. Alan Turing est connu tout autant pour sa « machine virtuelle » modèle fonctionnel de l'ordinateur que par ses travaux de décryptage du code des réseaux secrets allemands (Enigma) pendant la deuxième guerre mondiale. Entre les deux, machine virtuelle et décryptage, il y a d'ailleurs une homologie qui a été souvent soulignée : la machine de Turing fonctionne sur la capacité de dissimulation, de mensonge, de tromperie à dissiper pour réussir à identifier la différence entre l'intelligence humaine et la capacité de « penser » d'une machine. On sait aussi que le contenu de la question posée à la machine joue sur l'identité sexuelle du locuteur, mais ceci est un autre point, dont ne lui surent peu gré les autorités britanniques...

Le numérique s'est forgé dans les derniers conflits, depuis la deuxième guerre mondiale dans la manipulation et l'interception des données, dans la nécessité de casser des codes, dans la dissimulation des analyses.

Comme le montre le livre d'Isaac Ben Israël⁹, la logique du renseignement et celle de la recherche scientifique et de l'épistémologie sont fortement convergentes¹⁰.

Wikileaks a pu développer son projet aussi parce qu'Assange a particulièrement maîtrisé les outils de cryptages en jeu dans la protection des sources et des données.

Wikileaks est effraction du secret d'État, de la classification du secret défense. Par la protection des sources, il s'arroge un double pouvoir, sur l'ennemi politique, certes, mais aussi sur les médias, qui sont contraints de traiter avec lui.

En même temps qu'il protège l'anonymat du *Whistle blower*, il assure une plate-forme de mutualisation des sources, sorte de souveraineté publique implicite que la communauté numérique a intérêt à protéger, à préserver.

Le secret c'est le pouvoir, et le pouvoir, c'est le secret. « L'arcane est le signe du despotisme »¹¹. Le secret, est à l'origine nu, ou vision de l'effroyable, indicible, ouverture des portes sur les camps – c'est-à-dire sur l'anéantissement –, sur l'insondable des génocides. Derrière le secret défense et les documents classifiés, l'horreur, origine mystérieuse, ambivalente. Qui a tué Habyarimana au Rwanda ? Au moins deux versions possibles, peut-être indissociables. Enquête sans fin, analyse interminable.

Wikileaks et Anonymous s'inscrivent dans cette relation ambivalente au secret d'État, mais où tout est liquide, crypté, calculé, dévoilable et diffusable à l'infini. Que devient le secret d'État dans le cyberspace ? Production et croisement à l'infini des fichiers, informatique et liberté, profilage généralisé des identités, secret privé comme une peau de chagrin.

Le dévoilement à l'heure de l'ouverture des données, certes, mais en même temps, inversement, et peut-être paradoxalement, s'affirment des impératifs de contraintes supplémentaires : identifications, protection renforcée de secrets, appels à des technologies de cryptage plus élaborées, et sûrement nouvelles pratiques de dissimulation à la hauteur de ces nouveaux enjeux d'ouverture et de transparence. Tout un marché du secret tend à se développer sur Internet, en fonction des cercles d'initiés, des couches successives de pouvoirs, de propriété et de surveillance.

« Squelette dans le placard, tout le monde le sait, mais personne n'en parle, l'existence de moyens secrets de la politique est (re)devenue un secret, mais de Polichinelle. »¹²

⁹ Ben Israël, Isaac, *Philosophie du renseignement. Logique et morale de l'espionnage*, Paris, L'Éclat, 2003.

¹⁰ Ben Israël souligne aussi l'importance des archéologues (anglais en l'occurrence) dans le renseignement...

¹¹ Dewerpe, *op. cit.*, p. 77.

¹² Dewerpe, *op. cit.*, p. 89.

Le numérique, idéal de transparence, génère son propre secret, pour mieux le transgresser... Le vol de votre identité numérique peut faire maintenant l'objet d'une couverture assurantielle (Cf. la couverture du risque AXA !)

Comme le dit John Young dans *Cryptome* : "*Internet is a 'Vast Spying Machine'.*" Internet est à lui-même son propre espace d'espionnage. Tout étant sur Internet, ou du moins tout y étant caché, il faut des moteurs de recherche (de plus en plus focalisés) pour identifier et analyser les traces intéressantes, discriminer les copies pertinentes.

Globalement, il est important de ré-inscrire Wikileaks dans l'histoire politique des relations entre secret et transparence, entre « Lumière et opacité, entre droit et arbitraire », comme le fait Alain Dewerpe, même s'il faut en penser la spécificité numérique, la spécularité propre.

« La transparence trouve continûment une contrepartie dans l'usage plus ou moins raisonné du secret, de la dissimulation et de la tromperie, suivant des modes nouveaux qui découlent de la mise en œuvre historique du nouveau régime d'opinion publique : relation spéculaire ou, si l'on préfère, faces d'une même médaille »¹³.

Avec le cyberspace, le caché EST dans la révélation, dans l'amoncellement monstrueux des données. Comme dans ces dessins accumulant les détails « Où est Charlie ? », le caché est là sous les yeux, mais invisible. En tous cas sans moteur de recherche. La neutralité du Web, c'est la *Purloined letter* de Edgar Poe, la *Lettre volée*. Ce n'est pas le contenu qui compte, mais le fait qu'elle est là bien visible, crevant même les yeux, mais que la police, justement parce qu'elle la croit cachée, ne peut la voir ! Seul Dupin, par raisonnement logique démasque l'illusion et identifie la lettre, cachée dans le banal.

Le cyberspace est à la fois opacité et transparence, copie ambivalente, trahison et traduction du réel.

La révélation

Wikileaks par son dispositif de captage de source et de diffusion de fuites ressemble à celui de l'espionnage et du renseignement, où une puissance cherche à s'accaparer l'information sensible d'une autre puissance, ennemie. Mais ici la puissance d'origine est Internet comme puissance mondiale ouverte, et l'ennemi, ce sont des puissances mondiales étatiques qui violent les droits de l'homme et, au premier chef, la liberté d'expression du cyberspace.

¹³ Dewerpe, *op. cit.*, p. 90.

De ce point de vue, le dispositif est celui de la dénonciation, de la révélation où l'opinion publique mondiale est prise à témoin, sinon à partie.

Déjà, dans la sphère du renseignement, le dévoilement du secret est l'une des tendances : la gestion du secret nécessite qu'il y ait fuite, roman, rumeur, fiction, mémoires, ne serait-ce que pour témoigner de la puissance du secret public. Jamais la littérature de « témoignage » sur les affaires, scandales et autres complots d'État n'a été aussi dense. Jamais le secret n'a été aussi bavard.

Immanence du « complot numérique »

Corrélat de cette nouvelle relation numérique du secret et de la transparence, mais aussi de la prodigieuse force mémétique de réplication, la croissance de la croyance en la manipulation, au complot, signerait une nouvelle régression obscurantiste. Par le brouillage des frontières, le numérique devient-il le règne de l'illusion et de la ruse, de la fiction et de la tromperie¹⁴ ?

Si fuites et sources sont indissociables, dans la même explosion numérique ; si c'est au sein d'un même espace cybernétique que les données sont à la fois cryptées et dévoilées, la dialectique entre secret et transparence acquiert une dimension et une dynamique inédites, qui nous semble plutôt annuler le complot, comme souhaite le faire Wikileaks et Anonymous.

Aucun sens « caché » ne peut être invoqué comme source d'une action transcendante, dans la mesure où c'est forcément au sein de cet espace numérique que le secret s'exprime et court à tout instant le risque d'être dévoilé.

Le sens caché est potentiellement du dévoilé, et relève donc plus de la possibilité d'un imaginaire immanent des mondes possibles que de la croyance transcendante en une théorie du complot, supposant une instance manipulatrice.

Cette immanence expliquerait que l'espionnage, de caché, soit devenu une pratique de dévoilement, dont la finalité serait la liberté publique

Dans le cyberspace, le renseignement est le fait d'un espion double, triple, retourné, infiniment spéculaire. Tout dépend de l'arrêt sur image. L'Empire, s'il ne peut contrôler les fuites, tente de contrôler les circuits (numériques) bancaires, les sites d'hébergement, le *Cloud* planétaire, mais Wikileaks et d'autres acteurs du hacking continuent d'organiser la fuite.

Secret public, secret privé

¹⁴ Cf. Françoise Gaillard, « Quand le citoyen se complait dans le complot », *Libération*, 2 décembre 2010, <http://www.liberation.fr/monde/01012305698-quand-le-citoyen-se-complait-dans-le-complot>

A noter également que le secret d'État et le secret privé ne cessent de se rapprocher, d'interagir. Des affaires récentes ont montré à quel point la frontière entre vie privée (dans ses composantes les plus intimes, par exemple la sexualité) et la vie publique est poreuse ! Il n'est pas très étonnant que Julian Assange manifeste également cette porosité des composantes privées, avec les accusations de viol dont il est l'objet en Suède...

Wikileaks a besoin impérativement de cette face du dévoilement, de la révélation, de la dénonciation publique. Wikileaks s'introduit entre le secret d'État et les médias internationaux, alimentant par l'Internet l'opinion publique internationale. La force de réplication mondiale d'une source non identifiée est ici universellement prise à témoin. On comprend qu'Assange se soit très vite affronté au seul protagoniste à la hauteur de ce défi, l'Empire américain.

Moins de secret d'État, mais plus de secrets privés. Le secret de l'isolement. Le secret est également réintroduit pour des raisons d'efficacité (secret administratif), obligation de réserve ou de sûreté, sinon de situation d'exception (loi anti-terroristes). « La théorie politique sur laquelle s'est construit le droit libéral n'exclut pas qu'il faille mettre un voile sur la loi afin de défendre la liberté. (Montesquieu) ... une mise en réserve de la loi prévue, contrôlée et sanctionnée par la loi elle-même », nous rappelle Dewerpe¹⁵. Souhaitons qu'aucune exception à la loi ne soit imaginée à l'encontre de Wikileaks !

La duplication imaginaire de l'anonymat

Wikileaks et Anonymous alimentent fortement l'imaginaire de dévoilement du secret, là encore de façon ambivalente, d'un côté par l'individualisation forte, hypermédiatisée, voyante, provocante, d'Assange, de l'autre par l'anonymat des visages de Guy Fawkes, par l'uniformisation métallique de la voix d'Anonymous.

Cette duplication imaginaire de l'anonymat, au-delà de la figure charismatique du gourou libertaire Assange, est peut-être la création d'un espace sacré au sein du cyberspace : dramatisation d'une figure centrale, liée au secret et au pouvoir démiurgique du dévoilement, porte de l'icônostase, mais surtout également réplication des figures de l'anonymat (« Nous sommes légion, nous sommes partout, nous vous attendons... »). La véritable puissance de copie porte maintenant sur n'importe quel membre de la communauté du cyberspace, comme espace de liberté absolue d'information, sous le masque identique de Guy Fawkes, synthèse à la fois du plus protégé (anonymat du secret individuel) et diffusion la plus large de l'image du masque Anonymous en boucle sur YouTube ou dans les rues du monde.

¹⁵ Dewerpe *op. cit.*, p. 80.

Conclusion

Avec le numérique, et de plus en plus avec ce qui est nommé Big Data, la question de la transparence, liée à l'utilisation des données, devient capitale. Données publiques, Open access, autant d'exigences de transparence. Mais l'exemple de Wikileaks montre à l'envi combien complexe devient le rapport entre transparence et domaine réservé, données sensibles et conditions de leur divulgation. Devant le foisonnement des données disponibles, l'opacité peut provenir des algorithmes de traitement propres à les exploiter. La question de la qualité des données est également fort sensible. Avec le numérique, plus il y a transparence, et plus il y a secret. Et vice versa. À sa façon, Google capte, à travers les requêtes des utilisateurs de son moteur ou de Gmail, « tous les désirs du monde ». Les conditions d'utilisation des données dans un certain nombre de pays, dont la Chine, sont loin de respecter les droits de l'homme. À l'avenir, d'autres Wikileaks, avec d'autres modes opératoires devront casser le code, percer *l'arcana imperii*. La transparence du secret a de beaux jours devant elle...

La maîtrise des moyens numérique de recherche, donc de renseignement deviendra de plus en plus vitale, au risque sinon d'un Internet de l'amoncellement de copies illisibles, invisibles, sinon menaçantes. Est-il concevable par exemple que les règles de confidentialité des données soient édictées par Google, et non par la puissance publique, et laquelle ? Le combat pour la « neutralité » du Web sera essentiel, sinon un autre protocole, incarnant la neutralité « publique » devra émerger, dans une nouvelle clandestinité, une autre contre-culture.

En parallèle à ces nouvelles conditions de co-existence de la transparence et du secret, à une échelle globalisée encore jamais égalée, il y a fort à parier que l'imaginaire des possibles ne se renforce. La prédictibilité issue du Big Data sera peut-être à la fois plus ouverte et moins contrôlable, obligeant le « secret de polichinelle » numérique à faire ou laisser la place à de nouvelles formes du sacré et du caché, pour des formes inédites, et peut-être dégradées, de souveraineté publique.

Bibliographie

ASSANGE, Julian, *Essays on Conspiracy*, Cryptome, 2006, <http://www.cryptome.org/0002/ja-conspiracies.pdf>

BARDEAU, Frédéric, DANET Nicolas, « ANONYMOUS Peuvent-ils changer le monde ? », éd. FYP, 2011

BEN ISRAEL, Isaac, *Philosophie du renseignement*, Editions de l'Eclat, 2004

BOLTANSKY, Luc, *Énigmes et complots, Une enquête à propos d'enquêtes*, Paris, Gallimard 2012

- COHEN TANOUDJI, Laurent, « Le clair obscur d'Internet », *Revue, Pouvoirs*. Numéro 97, 2001/2, « Transparence et secret », p. 85-90
<http://www.revue-pouvoirs.fr/-97-Transparence-et-secret-.html>
- DEWERPE, Alain, *Espion. Une Anthropologie historique du secret d'État contemporain*, Paris, Gallimard, 1994
- DOMSCHEIT-BERG, Daniel, *Inside Wikileaks*, Paris, Grasset, 2011
- FORCADE, Olivier, LAURENT, Sébastien, *Secrets d'État, Pouvoir et renseignement dans le monde contemporain*, Paris, Armand Colin, 2005
- GAILLARD, Françoise, « Quand le citoyen se complait dans le complot », in *Libération*, 2 décembre 2010,
<http://www.liberation.fr/monde/01012305698-quand-le-citoyen-se-complait-dans-le-complot>
- LEIGH David, HARDING, Luke, *Wikileaks la fin du secret*, Original Books, 2011
- PREMAT, Christophe, « L'effet Wikileaks », in *Sens Public*, juin 2011,
<http://www.sens-public.org/spip.php?article848>
- RIVIERE, Philippe, « WikiLeaks, mort au messager », in *Le Monde Diplomatique*, janvier 2011,
<http://www.monde-diplomatique.fr/2011/01/RIVIERE/20058>
- ROUDINESCO, Élisabeth, « La dictature de la transparence », in *Libération*, 2 décembre 2010,
<http://www.liberation.fr/monde/01012305697-wikileaks-la-dictature-de-la-transparence>
- STADLER, Félix, « Pourquoi les institutions peinent à conserver leurs secrets », in *Le Monde diplomatique*, Janvier 2011
- « The Media World after WikiLeaks and News of the World », 16-17 February 2012,
<http://www.unesco.org/new/en/communication-and-information/events/calendar-of-events/events-websites/the-media-world-after-wikileaks-and-news-of-the-world/>
- Owni <http://owni.fr/>
- « La Quadrature du Net », <http://www.laquadrature.net/>
- Wikipedia. Article : « Fuite d'information »
- WORMSER, Gérard, « Banco !... L'espace public à l'heure du numérique », in *Sens Public*, décembre 2010, <http://www.sens-public.org/spip.php?article800>