

Surveillance numérique et raison d'Etat : doit-on tout savoir ?

Pierre Schweitzer

▶ **To cite this version:**

Pierre Schweitzer. Surveillance numérique et raison d'Etat : doit-on tout savoir ?. 2018. hal-02120797

HAL Id: hal-02120797
https://amu.hal.science/hal-02120797

Preprint submitted on 6 May 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Copyright

Surveillance numérique et raison d'Etat : doit-on tout savoir ?

Introduction :

La collection d'informations par le prince est sûrement aussi vieille que la notion d'Etat elle-même. La police de Fouché, à l'époque napoléonienne, a constitué un tournant en France dans la constitution de services de renseignement modernes et bien organisés. Aujourd'hui la communication gouvernementale autour de la surveillance des communications dans les démocraties modernes met en avant la sécurité des citoyens eux-mêmes contre les menaces nombreuses qui vont des réseaux criminels crapuleux aux groupes terroristes, sans oublier les risques géopolitiques allant de la lutte contre l'influence étrangère hostile (on ne peut s'empêcher de penser aux accusations portées par de nombreuses démocraties occidentales contre les efforts d'influence active de la Russie) jusqu'au risque d'invasion militaire du territoire national. Comme dans toute entreprise humaine, les criminels ont besoin de coordonner leurs efforts et utilisent pour cela des moyens de communication modernes. L'interception de messages à l'intérieur de ces réseaux permet d'identifier les malfaiteurs, de connaître leurs projets criminels, leurs motivations, leur localisation, et de collecter des éléments de preuves pour alimenter une procédure judiciaire après leur arrestation par les autorités.

Après plusieurs décennies de présence croissante des technologies informatiques dans toutes les couches de nos sociétés occidentales, nous commençons à disposer d'un recul suffisant pour tenter d'analyser les effets de la révolution numérique sur notre rapport à l'Etat. La question du terrorisme qui sévit depuis 2001 sous des formes sans cesse renouvelées a soulevé un débat sur la réponse publique à adopter en matière de surveillance des communications numériques, ainsi que les limites qu'il convient d'apporter à ce pouvoir dans le cadre d'une démocratie libérale dont la plupart des pays occidentaux se réclament. Le problème du terrorisme n'est certes pas nouveau, puisque des anarchistes de la fin du 19ème siècle aux islamistes d'aujourd'hui, en passant par l'OAS, les mouvements indépendantistes dans les colonies puis en métropole, la France n'a connu que peu de répit. Mais la conjugaison entre des réseaux de communication de plus en plus libres et décentralisés, le poids croissant de l'Etat dans la société (qu'on mesure notamment par le poids désormais majoritaire de la dépense publique), la surmédiatisation de la violence dans une société où les citoyens tolèrent de moins en moins le risque, fait que le débat public sur la surveillance semble plus vif que jamais. Comment on pouvait s'y attendre, les technologies numériques ont été à la fois un nouveau moyen pour l'Etat de surveiller ses administrés, mais parfois aussi pour les administrés de surveiller leur Etat. Deux affaires très médiatiques l'ont parfaitement illustré, et serviront de base à notre réflexion : d'abord les révélations de l'organisation Wikileaks, puis les documents rendus publics par Edward Snowden (voir encadré). Dans des pays de tradition démocratique comme la France, les Etats-Unis ou la Grande-Bretagne, il est communément accepté que l'Etat est une émanation de la volonté des citoyens, et que ce dernier doit se borner à assurer son mandat dans un cadre législatif bien établi. Autrement dit l'Etat garantit aux citoyens l'exercice de leur liberté, mais cette dernière pré-existe à l'Etat, comme le précisent la plupart des constitutions modernes. Or nous assistons depuis le début du 21ème siècle à un renversement de cette situation où désormais l'Etat tend à outrepasser sa propre législation, tout en resserrant dans le même temps son contrôle de l'activité des citoyens. Partant de là, nous nous demanderons si ces dérives par-delà la frontière du droit sont justifiables par le contexte terroriste, avant de nous interroger sur les moyens de nous prémunir du risque de dérive autoritaire dans les décennies à venir.

Etat des lieux de la surveillance exercée par les autorités publiques

Accroissement et changement de logique de la surveillance des communications électroniques

Depuis la chute des totalitarismes du 20ème siècle, les démocraties libérales gèrent la question du renseignement selon une logique assez bien définie et communément acceptée. L'Etat et ses agences peuvent exercer une surveillance des communications privées entre individus dans des cas précis et avec l'autorisation du pouvoir judiciaire, qui agit alors comme contre-pouvoir au sein-même de l'Etat. Si le pouvoir exécutif dispose d'éléments permettant de soupçonner un citoyen d'actes criminels, particulièrement des actes terroristes, les représentants du pouvoir judiciaire sont saisis du dossier et peuvent autoriser des écoutes ou d'autres modalités d'interception des communication, en collaboration avec les opérateurs privés de télécommunications qui sont soumis à la législation nationale. Mais à la suite des attentats du 11 septembre 2001 aux Etats-Unis, le gouvernement américain dirigé par Georges W. Bush a fait voter au Congrès le Patriot Act, un paquet législatif qui a brusquement étendu les pouvoirs de l'exécutif au détriment du judiciaire dans les enquêtes liées à des actes de terrorisme, ainsi que dans des activités considérées comme possiblement liées à des réseaux terroristes. Le ralliement massif de l'opinion américaine, toutes tendances politiques confondues, autour de son Etat, a conforté les gouvernements successifs dans l'idée que la fin - vaincre le terrorisme - justifiait les moyens, en l'occurence la perte de certaines libertés au bénéfice d'une plus grande sécurité. Bénéficiant dès lors de moyens financiers largement accrus, de l'appui de l'opinion publique et de l'aval du gouvernement, les agences publiques chargées du renseignement ont cherché à faciliter leur travail en inversant la logique qui avait prévalu jusqu'alors. C'est donc dans le cadre de la "guerre contre le terrorisme" que les renseignements ont patiemment bâti un système de collecte généralisée des communications électroniques. Les techniques modernes sont bien différentes de l'image d'Epinal de l'opérateur avec son casque vissé sur les oreilles, écoutant attentivement la conversation téléphonique des bandits présumés, carnet de notes et crayon à la main. A l'ère de l'analogique il eut été infaisable, humainement et financièrement, d'enregistrer sur des bandes magnétiques la totalité des conversations téléphoniques en vue de conserver ces enregistrements pour une possible utilisation future. Et même si l'on avait pu tout stocker, l'exploitation n'aurait pu reposer sur sur une écoute "manuelle". L'effondrement du coût et des capacités de stockage et de calcul des outils informatiques a profondément changé la donne. De même que Google et ses concurrents maîtrisent parfaitement la compréhension du contenu de milliards de sites web qu'ils indexent ensuite avec une pertinence étonnante compte-tenu de leur mode de fonctionnement largement non-humain, les mêmes techniques d'exploitation automatisée de contenus textuels (e-mails), mais aussi audiovisuels (détection de personnes et d'objets dans les photos et vidéos, reconnaissance vocale et traduction automatique) sont à la portée des institutions de pays développés technologiquement avancés et prêts à y consacrer des budgets de plus en plus conséquents. L'essor fulgurant de l'intelligence artificielle de type "deep learning", ou "machine learning", dotée de capacités d'apprentissages qui émulent le fonctionnement d'un vrai réseau de neurones, ne peut que faciliter l'exploitation de ces données nombreuses et variées. Du point de vue des institutions chargées du renseignement, on peut raisonnablement imaginer que l'idée d'une totale transparence des communications des citoyens est regardée avec envie. C'est d'ailleurs pour cela que les démocraties modernes disposent systématiquement de contre-pouvoirs face à ceux qui sont responsables de la sécurité, et dont l'envie de réussir dans leur mission peut naturellement les rendre sensibles à l'idée commune selon laquelle si un citoyen n'a rien à cacher, il n'a dès lors rien à craindre.

Voici donc réunies trois conditions essentielles pour la mise en place d'une surveillance généralisée des communications : la capacité technique à opérer la collecte et l'exploitation des données concernées, l'existence d'un risque terroriste majeur dont la puissance publique peut légitimement

s'inquiéter, et un soutien dans l'opinion publique des pays concernés à la mise en place de mesures de surveillance plus fortes qu'auparavant, au moins temporairement. De quels indices disposons-nous, dès lors, pour appuyer l'hypothèse d'un renversement de logique en faveur d'une surveillance non plus limitée aux seuls suspects, mais véritablement généralisée ? Les exemples étant nombreux, nous nous limiterons à ceux qui nous semblent les plus pertinents. Les informations proviennent de sources diverses : anciens collaborateurs d'agences de renseignement gouvernementales, communiqués et rapports officiels rapports de ces mêmes agences, activistes militant dans diverses ONG, entreprises privées ayant fait l'objet de requête de la part des services de renseignement, ainsi que d'anciens employés de ces mêmes entreprises. Si dans un premier temps nous avons pu penser que les Etats-Unis étaient plus avancés que les pays européens sur la voie de l'inquisition numérique, la succession de la Loi Renseignement du 24 juillet 2015 en France et de l'Investigatory Powers Act du 29 novembre 2016 au Royaume-Uni a montré combien l'Europe imite les Etats-Unis à quelques années d'écart.

Penchons-nous d'abord sur les révélations d'Edward Snowden (voir encadré), ancien collaborateur contractuel travaillant sur des projets de la NSA, qui a contacté en 2013 des journalistes d'investigation reconnus pour leur transmettre des documents mettant au jour plusieurs programmes secrets de collecte massive de données privées aux Etats-Unis et ailleurs dans le monde. Plusieurs auditions officielles ont suivi ces révélations, au cours desquelles plusieurs représentants des différentes composantes du renseignement américain ont justifié les programmes de surveillance dont les documents fournis par Snowden ont pu prouver l'existence. Les documents ont notamment montré que la collecte massive démarrée sous l'administration de Georges W. Bush et dont son successeur Barack Obama avait annoncé l'arrêt en 2011[1] avait en réalité continué depuis[2]. La NSA en particulier s'est défendue en affirmant son respect des limites légales posées par la cour Fisa, la cour secrète de justice chargée de fixer le cadre de la collecte de données pour le renseignement extérieur. Plusieurs membres du congrès se sont inquiétés que la NSA ait le pouvoir d'estimer elle-même si les décisions de la Fisa étaient respectées, sans possibilité de contrôle extérieur. Des membres du Congrès se sont également émus que la NSA soit en mesure de collecter des méta-données. La surveillance des méta-données signifie que les services de renseignements, bien que ne disposant pas forcément de l'accès au contenu d'une conversation audio ou d'un e-mail, collectent néanmoins les identités des émetteurs, récepteurs, leur localisation, la durée de l'échange, ainsi que dans certains cas les appareils utilisés, la présence et la nature des pièces jointes dans un e-mail, etc. Certains spécialistes tels que Bruce Schneier ou Susan Landau estiment que les méta-données sont souvent aussi informatives que les contenus des échanges, ce qui fait de leur collecte une forme d'intrusion comparable à l'écoute téléphonique ou la lecture de courriers. Sont surveillés par la NSA non seulement les terroristes suspectés, mais également leur entourage, l'entourage de leur entourage, et même l'entourage de l'entourage de leur entourage (*three-hop analysis*). Ce qui signifie concrètement, d'après les données dont nous disposons, qu'une personne soupçonnée de sympathies terroristes peut légalement entraîner la surveillance de ses 190 contacts Facebook (moyenne fournie par le réseau social), ce qui au second degré entraîne la surveillance d'environ 30.000 personnes, et plus de 5 millions de personnes au troisième niveau.[3]

---

[1] Shawn Turner, directeur de la communication de l'administration Obama en matière de renseignement fédéral, avait déclaré au quotidien The Guardian : "Le programme de collecte de méta-données autorisé par le tribunal Fisa a été arrêté en 2011 pour des raisons opérationnelles et des questions de ressources, et n'a pas été redémarré depuis"

[2] Glenn Greenwald et Spencer Ackerman dans The Guardian (27 juin 2013) montrent que non seulement le programme ne s'est pas arrêté comme l'affirmait Shawn Turner, mais que la moitié du volume total de données collecté depuis son démarrage l'avait été pour la seule année 2012. https://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection

[3] The Guardian, 28 octobre 2013. https://www.theguardian.com/world/interactive/2013/oct/28/nsa-files-decoded-hops

Suite à la tuerie de San Bernardino en 2015, revendiquée par des terroristes affiliés à l'Etat Islamique, le FBI s'est adressé à l'entreprise Apple pour déchiffrer les données contenues sur les téléphones du couple d'assassins, deux iPhone. Apple a refusé de collaborer tant qu'elle ne serait pas mise en face d'une procédure judiciaire en bonne et due forme, et a rappelé qu'elle n'avait plus la capacité technique de déchiffrer elle-même les données concernées. C'était justement suite à des demandes nombreuses émanant des autorités qu'Apple avait décidé, bien avant la tuerie de 2015, de se couper d'une telle possibilité, invoquant la sécurité et la vie privée de ses clients. En effet, si les entreprises qui reçoivent ces "gag letters" (lettres des autorités demandant qu'on communique des données concernant leurs clients) n'ont pas l'autorisation d'en informer quiconque, Apple avait tout simplement fait disparaître une phrase qui figurait dans ses précédents rapports annuels, et qui indiquait que l'entreprise n'avait pas encore été sommée de communiquer des données. L'ensemble de l'industrie avait alors compris le message : Apple recevait désormais des requêtes en informations sans avoir le droit d'en informer ses clients[4]. Le FBI a obtenu par la suite une décision judiciaire demandant la déchiffrement des téléphones, à laquelle Apple a préféré ne pas répondre tant que les recours judiciaires le lui permettaient[5]. L'affaire était surtout symbolique selon les experts, puisque le FBI n'a finalement pas eu besoin d'Apple pour débloquer et déchiffrer les téléphones, mais a pu montrer publiquement à cette occasion qu'Apple refusait en l'état leur demande de collaboration. La requête était d'ailleurs plus large : le FBI demandait pour l'avenir à disposer d'une "backdoor" (porte dérobée) dont lui seul détiendrait la clé et qui lui permettrait d'accéder au contenu de n'importe quel iPhone pour les besoins d'une enquête, y compris à distance.
Plus récemment, en octobre 2016, l'entreprise Yahoo, notamment connue pour son service de courrier électronique qui compte encore près de 280 millions d'utilisateurs, est épinglée par l'agence Reuters pour avoir installé un logiciel espion à la demande de la NSA et/ou du FBI. Le logiciel, installé à l'insu de l'équipe de sécurité Yahoo, serait le premier cas documenté de surveillance massive des communications en temps réel sans discrimination sur les individus surveillés, alors que le programme PRISM concernait plutôt des discussions archivées et s'appuyait sur les moyens techniques de la NSA[6].

Les agences de renseignement américaines - on peut raisonnablement l'affirmer d'après les éléments avérés - ont donc fait du zèle en matière de surveillance au détriment de l'esprit du 4ème amendement de la constitution américaine. Les américains ne sont d'ailleurs pas les principaux concernés, puisque le 4ème amendement complique le travail de surveillance systématique sur des citoyens des Etats-Unis, et que les agences comme la NSA concentrent donc leurs efforts sur les étrangers et les américains en contact avec des étrangers considérés comme intéressants à surveiller. Michael V. Hayden, directeur de la Central Intelligence Agency (CIA) entre 2006 et 2009 le résume ainsi dans un article paru dans la foulée des révélations d'Edward Snowden : "Je vais vous le dire de la manière la plus abrupte. Le renseignement américain est limité par les exigences du 4ème amendement et défini par les exigences de la sécurité américaine. En l'absence de directives politiques contraires, si vous n'êtes pas couvert par la constitution américaine, et que vos communications contiennent des informations pouvant contribuer à la liberté et à la sécurité de l'Amé-

[4] Cette pratique est surnommée « warrant canary » par les anglo-saxons, en référence à la présence historique de canaries dans les mines de charbon pour avertir de la raréfaction d'air respirable avant qu'il ne soit trop tard. C'est à partir du rapport suivant que l'entreprise Apple a changé la formule qui faisait office de warrant canary, ouvrant des spéculations sur les requêtes gouvernementales secrètes reçues par l'entreprise
https://www.apple.com/legal/privacy/transparency/requests-20131231-en.pdf
[5] Il ne s'agissait pas à proprement parler d'un mandat, mais d'une ordonnance d'un tribunal californien (United States District Court for the Central District of California) consultable à cette adresse : https://assets.documentcloud.org/documents/2714005/SB-Shooter-Order-Compelling-Apple-Asst-iPhone.pdf
[6] The Guardian, 5 octobre 2016 https://www.theguardian.com/technology/2016/oct/04/yahoo-secret-email-program-nsa-fbi

rique, informations qui ne seraient pas autrement mises à la disposition du gouvernement des Etats-Unis, alors on fonce. Le directeur de la NSA n'a que faire de votre vie privée."[7]

En est-il de même en France ? Pour Claudine Guerrier, auteure en 2009 d'un rapport riche d'enseignements sur la surveillance des communications face au droit, le tournant observé après 2001 aux Etats-Unis s'est retrouvé dans la majorité du monde occidental. Si les deux dernières décennies du 20ème siècle avaient été marquées par l'émergence d'institutions de contrôle et autres contre-pouvoirs à la surveillance des communications privées, c'est au contraire une idéologie sécuritaire qui prévaut depuis le début du 21ème siècle et jusqu'à aujourd'hui. En France comme ailleurs, il est frappant de constater combien la mise en place d'un cadre légal pour la surveillance des communications fait souvent suite à des scandales portant sur l'abus de cette pratique par le pouvoir exécutif. Ce fut le cas avec le scandale du Watergate aux Etats-Unis, et l'instauration de la Cour spécifique prévue dans le FISA Act qui le suivit. En France le scandale dit des "écoutes de l'Elysée" sous la présidence de François Mitterrand a finalement abouti à la loi du 10 juillet 1991. Cette dernière pose clairement le secret des correspondances comme règle générale, et prévoit les "interceptions administratives" dans des cas relevant de l'atteinte à la sécurité nationale, la prévention des actes de terrorisme, la prévention de certains crimes et délits, l'atteinte au patrimoine scientifique et économique. Les ministères de la Défense, de l'Intérieur et celui dont dépendent les douanes peuvent en faire la demande au premier ministre qui a la liberté de les autoriser ou non pour une durée de 4 mois renouvelables. Cette loi entérine également la création de la Commission Nationale de Contrôle des Interceptions de Sécurité (CNCIS), qui a le pouvoir d'émettre des avis consultatifs sur les demandes d'interceptions administratives de sécurité, que le premier ministre choisit ou non de suivre. Suite au choc mondial des attentats du 11 septembre 2001, on constate une volonté de renforcer les outils de surveillance, ce qui a été fait dans la loi du 9 mars 2004 dont l'un des objectifs est la "mise en place de moyens d'investigation supplémentaires pour les officiers de police judiciaire (concernant l'infiltration des réseaux, les écoutes téléphoniques, la perquisition et la garde à vue)"[8]. Le 23 juillet 2006 une autre loi vient renforcer le pouvoir des services de renseignement avec l'obligation faite aux opérateurs télécoms de transmettre de nombreuses données conservées sur l'activité de leur abonnés, mais toujours avec un contrôle exercé par la CNCIS. La même année, au niveau de l'Union Européenne, la directive « Data Retention »[9] permet de conserver les paramètres techniques pendant une durée qui va de six à vingt-quatre mois. Comme pour les précédentes "couches" législatives, cette directive va dans le sens d'un contrôle renforcé des communications privées, avec un champ d'application si large que la Cour de Justice de l'Union Européenne a invalidé la directive sur la conservation des données de connexion par un important arrêt du 8 avril 2014, estimant que la directive « comporte une ingérence dans [les] droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire ».

---

[7] "Let me put this in the starkest possible terms. American signals intelligence is limited by the demands of the Fourth Amendment and defined by the demands of American security. Absent political guidance to the contrary, if you are not protected by the US Constitution, and your communications contain information that would help keep America free and safe, information that would not otherwise be made available to the US government, then game on. Your privacy is simply not the concern of the NSA director." Extrait d'un article de Michal V. Hayden, ex-directeur de la CIA, paru en janvier-février 2014 dans la revue World Affairs.
http://www.worldaffairsjournal.org/article/beyond-snowden-nsa-reality-check

[8] Site internet de la Direction de l'information légale et administrative. http://www.vie-publique.fr/actualite/panorama/texte-vote/loi-du-9-mars-2004-portant-adaptation-justice-aux-evolutions-criminalite.html

[9] Directive 2006/24/CE, dite "Data retention".

Cette volonté d'accroitre la surveillance se traduit d'ailleurs dans les faits, puisque Claudine Guerrier, dont le grand rapport date de 2009, dresse le constat suivant : "Qu'il s'agisse des interceptions traditionnelles (téléphone, mél) ou des données techniques, il est évident que les organismes de contrôle semblent amoindris depuis le début du vingt-et-unième siècle, bien que, dans certains cas, des entités de contrôle soient créées dans le cadre de lois plus ou moins liberticides. L'équilibre entre vie privée et sécurité penche, pour les organismes de contrôle comme pour les autres acteurs, en faveur de la sécurité."[10] Les chiffres communiqués par les pouvoirs publics ont suscité un nombre d'articles conséquent dans la presse française, qui note que le nombre des interceptions judiciaires a explosé de plus de 440 % en sept ans, passant de 5 845 en 2001 à 26 000 en 2008[11]. Il faut y ajouter les 5096 interceptions administratives réalisées en 2008. On peut néanmoins relativiser ces statistiques par le fait que la France était nettement en dessous de ses voisins en termes de surveillance des communications au début des années 2000. La dynamique traduit pourtant une volonté réelle, affichée, de recourir plus largement à la surveillance des communications. Dans le même esprit, on notera la mise en place progressive d'un réseau de satellites que les anglo-saxons ont surnommé "Frenchelon". "Censé servir à collecter des informations pour la Défense nationale, afin de prévenir les conflits, lutter contre le terrorisme et la prolifération des armes nucléaires, ce réseau est soupçonné d'espionnage économique", d'après Claudine Guerrier. Soulignant que ces interceptions ne font l'objet d'aucun contrôle émanant d'organisme indépendant, l'étude de 2009 évoque une "menace pour la vie privée".

Depuis 2001 nous sommes donc sur une pente sécuritaire assumée, qu'on peut analyser comme une réponse aux inquiétudes des citoyens et des gouvernements face à un terrorisme d'un genre nouveau, à la fois barbare dans ses attaques et parfaitement moderne dans son organisation criminelle, particulièrement pour ses communications internes et externes (recours aux réseaux sociaux, au messageries chiffrées sécurisées, etc.). Considérant cette réponse sécuritaire face à des attentats qui n'ont pas directement touché la France dans la première partie du 21ème siècle, on ne pouvait que s'attendre à une réponse toujours plus sécuritaire depuis que notre pays a subi une vague d'attentats historique débutée en janvier 2015 (attaque du journal Charlie Hebdo et d'un hypermarché cacher à Paris), et poursuivie en novembre 2015 (massacre lors d'un concert au Bataclan à Paris) puis en juillet 2016 (attaque de la Promenade des Anglais à Nice). D'un point de vue législatif, cette inflexion sécuritaire a pris la forme de la Loi Renseignement du 24 juillet 2015, qui propulse la France dans une nouvelle forme de surveillance non plus ciblée mais beaucoup plus large, préalablement à une exploitation ciblée des données collectées.

Des techniques de recueil de renseignements aujourd'hui permises dans un cadre judiciaire sont étendues au services de renseignement : balisage de véhicule, sonorisation de lieux privés (micros), captation d'images dans des lieux privés, captation de données informatiques, accès aux réseaux des opérateurs de télécommunications pour le suivi d'individus identifiés comme présentant une menace terroriste. Si la forme définitive de cette loi aboutit à une situation de surveillance considérablement renforcée, le projet initial du gouvernement de Manuel Valls était encore plus sécuritaire, par exemple dans sa volonté d'installer des mouchards sur les réseaux des fournisseurs d'accès à Internet (on les a souvent désignés sous le terme de "boîtes noires") afin de collecter des méta-données et de les exploiter de manière semi-automatisée pour détecter les comportements suspects, soit l'équivalent de ce que la NSA pratique déjà aux Etats-Unis. Devant les réticences des professionnels des télécoms et d'une partie du Parlement, le gouvernement a dû se résoudre à laisser les FAI s'occuper eux-mêmes d'opérer la séparation entre les méta-données (collectées par les services de renseignement à l'aide des boîtes noires) et les contenus corres-

[10] "Synthèse d'une étude de droit comparé en matière d'organismes de contrôle des interceptions de télécommunication", par le Professeur Claudine Guerrier, Institut Telecom/TSMP (ex-INT)/ CE-MANTIC, 2009.

[11] Christophe Cornevin dans Le Figaro, 27 juillet 2009. http://www.lefigaro.fr/actualite-france/2009/07/27/01016-20090727ARTFIG00412-les-grandes-oreilles-amplifient-les-ecoutes-.php

pondants (toujours protégés en règle générale par le secret des correspondances). De même, l'Assemblée nationale a limité l'utilisation des imitateurs d'antennes relais (IMSI catcher) - qui permettent d'aspirer les conversations dans un périmètre donné - à des agents individuellement désignés et habilités. L'intervention de l'Assemblée Nationale a aussi permis de corriger des motifs trop vagues qui auraient pu justifier la surveillance de manière très large, ainsi le motif "prévention des violences collectives de nature à porter gravement atteinte à la paix publique" a été remplacé par "prévention des atteintes à la forme républicaine des institutions et des violences collectives de nature à porter atteinte à la sécurité nationale". On pourrait ainsi multiplier les exemples de points sur lesquels le gouvernement a été limité dans ses velléités sécuritaires. Ce qui peut paraître relever du détail est tout à fait révélateur de l'état d'esprit du pouvoir exécutif qui, sans un contrôle des deux autres pouvoirs et des instances administratives indépendantes, semble souhaiter toujours plus de surveillance, au moins pour les principales formations politiques françaises qui se sont partagé le pouvoir pour l'essentiel de la V^{ème} République.

Au total, si on tient compte des déclarations officielles des agences de renseignement, ldes témoignages des entreprises de télécommunications, de leurs anciens employés, ainsi que d'autres sources que la presse la plus sérieuse considère comme fiables, on arrive à la conclusion tout à fait prévisible que les agences de renseignement, dans le monde entier, agissent constamment pour étendre le spectre de leur surveillance, sa profondeur et la souplesse juridique avec laquelle elles peuvent y procéder.

Hier et aujourd'hui, bénéfices et risques de la surveillance des communications par l'Etat et ses agences

De ce point de vue, et même si la polémique est vive au sujet de l'efficacité réelle de la collecte d'informations par les autorités, chacun pourra raisonnablement admettre qu'une surveillance plus étendue a de très fortes chances de faciliter le travail de la police et de la justice. A moins de souscrire à une théorie du complot, comment expliquer – sinon par une réelle efficacité attendue – la volonté des responsables de notre sécurité de disposer de pouvoirs de surveillance toujours plus large ? Si on peut être tenté de s'arrêter à ce constat pour souscrire au principe d'une surveillance étendue au nom d'une efficacité accrue, c'est au contraire à ce stade précis que notre analyse nécessite un approfondissement.

Malgré le choc immense dans l'opinion française des attentats islamistes de 2015, le débat public sur la Loi Renseignement fut beaucoup plus vif que lors des précédentes lois comparables. Et ce malgré le discours du gouvernement pour qui cette loi était la seule réponse possible compte-tenu du nouveau contexte d'insécurité. Ainsi les critiques sont venues de nombreuses ONG telles que La Quadrature du Net, Human Rights Watch, Reporters Sans Frontières, la Ligue des Droits de l'Homme, etc. Les professionnels du numérique se sont également fait entendre, plus de 600 d'entre eux se sont associés au sein de l'initiative baptisée "Ni pigeons, ni espions", dans l'espoir d'infléchir le projet de loi du gouvernement[12]. Le pouvoir judiciaire s'est aussi mobilisé par le biais d'organisations comme le Syndicat de la Magistrature, l'USM, l'Ordre des Avocats de Paris, et d'anciens juges anti-terroristes comme Marc Trévidic ou Alain Marsaud, ce dernier allant jusqu'à déclarer : « Avec un tel texte, toutes les oppositions, même politiques, peuvent être surveillées. »[13]

On notera que si les critiques de certains activistes du net et autres ONG traditionnellement hostiles à de telles législations étaient prévisibles, d'autres critiques étaient plus inattendues. Conscient de la réticence d'une partie de l'opinion, le gouvernement a donc voulu rassurer les oppo-

[12] Le Monde, 22 avril 2015. http://www.lemonde.fr/pixels/article/2015/04/22/ni-pigeons-ni-espions-les-acteurs-du-numerique-mobilises-contre-la-loi-sur-le-renseignement_4619971_4408996.html
[13] La Croix, 31 mars 2015. http://www.la-croix.com/Actualite/France/Loi-sur-le-renseignement-bientot-tous-surveilles-2015-03-31-1297227

sants en proposant une réforme de l'autorité administrative chargée de contrôler les interceptions de sécurité. C'est ainsi que la CNCSI est remplacée par la Commission de contrôle des techniques du renseignement (CNCTR), un changement qui s'accompagne de réformes dans le fonctionnement de cette autorité afin de respecter un équilibre entre pouvoir de contrôle et efficacité des dispositifs de surveillance. Mais à y regarder de plus près, on voit bien se dessiner un renforcement de la surveillance, et dans le même temps un affaiblissement *de facto* des contrôles et autres garde-fous. Ainsi Jean-Marie Delarue, dernier président de la CNCSI, a exprimé ses inquiétudes quant à l'affaiblissement du contrôle démocratique sur les services de renseignement, raison pour laquelle il n'a pas souhaité être associé à la future CNCTR[14]. Face aux députés de la Commission de la Défense, il a tenu des propos sans ambigüité : "pour fréquenter les services depuis des années, je sais que ces gens font un métier formidable et difficile, mais aussi que le principe de véracité n'est pas ce qu'ils apprennent en priorité. (…) Dans le projet de loi, aucune disposition ne prévoit un tri entre les mauvaises données et les bonnes. (…) L'un des services de ce pays dispose de moyens informatiques extrêmement puissants. J'en suis ravi. Mais lorsque nous allons voir ses instruments, notre intervention relève plus de la contemplation que de l'investigation. Si je dis à ce service que j'ai besoin d'aller voir ce qu'il fait, il va me bâtir un logiciel pour répondre à ma demande. Comment vérifier que ce logiciel répond effectivement à ma demande ? (…) Vous ne donnez pas à la CNCTR les moyens d'avoir prise sur les données brutes du contrôle, vous bâtissez un colosse aux pieds d'argile. Étant un peu expert en matière de contrôle depuis quelques années, je me permets de vous le dire. Si le contrôleur n'a pas accès aux données, il ne contrôlera que ce que l'on voudra bien lui donner et qui ne correspondra pas à la réalité. (…) Nous sommes bien dans la pêche au chalut chère aux Américains. (…) L'anonymat devient le seul moyen de protéger les libertés individuelles dans un contexte où nous sommes passés à la pratique de la pêche au chalut".[15] Ces craintes sont partagées par d'autres émanations de l'autorité publique, telles que le Conseil National du Numérique : "le Conseil est préoccupé par l'introduction de nouvelles techniques de renseignement, dont certaines peuvent confiner à une forme de surveillance de masse. (…) Cette approche a démontré son extrême inefficacité aux Etats-Unis en dépit d'investissements astronomiques."[16] Jacques Toubon, le Défenseur des Droits, souhaitait l'ajout de mécanismes de contrôle au projet de loi pour éviter les dérives. La CNIL, quant à elle, a exprimé de vives inquiétudes, dont certaines persistent malgré les changements apportés au projet de loi lors de son adoption définitive. [17]

S'il y a bien une leçon que nous pouvons tirer de l'étude des Etats modernes, en particulier depuis la fin du 18ème siècle, c'est que le renseignement a constamment été utilisé par le régime en place non seulement pour garantir la sécurité des sujets ou citoyens qui dépendent de lui, mais tout autant pour assurer sa propre survie en tant que régime politique. Nul besoin de remonter très loin dans l'histoire des grandes démocraties actuelles pour s'apercevoir que les "intérêts fondamentaux de la Nation" peuvent dangereusement se confondre avec les intérêts fondamentaux de l'Etat, parfois au détriment des intérêts de ses propres citoyens. Pour des raisons évidentes, mêmes les régimes aujourd'hui considérés à juste titre comme des dictatures, au premier rang desquels l'Etat

[14] Jean-Marie Delarue répondait aux questions du journaliste Marc Rees, le 21 septembre 2015, dans le journal NextInpact : « Le mois dernier, j'ai demandé à ne pas figurer parmi les membres proposés par le vice-président du Conseil d'État. Disons que s'il avait voulu penser à moi, je l'en ai dissuadé, parce que je pense que la loi sur le renseignement d'une part, et les techniques de saisine des données d'autre part, ne me donnent pas les garanties d'un contrôle suffisant. Par conséquent, je ne souhaite pas m'y associer. » http://www.nextinpact.com/news/96585-loi-renseignement-actuel-president-cncis-reitere-ses-doutes-et-critiques.htm

[15] Propos rapportés par La Tribune, 2 avril 2015. http://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/quand-le-gendarme-des-ecoutes-fusille-la-loi-sur-le-renseignement-de-valls-465876.html

[16] Communiqué de presse, 19 mars 2015. http://cnnumerique.fr/renseignement/

[17] A lire sur le site internet de la CNIL, 19 mars 2015. https://www.cnil.fr/fr/publication-de-lavis-sur-le-projet-de-loi-relatif-au-renseignement

Français (régime de Vichy) ou les pires totalitarismes fascistes et communistes du 20ème siècle, ont systématiquement invoqué la défense des intérêts et de la sécurité du peuple pour justifier leurs méthodes de surveillance totalitaires. Les historiens ont démontré que les moyens de l'Etat étaient en fait surtout utilisés pour garantir la perpétuation de la dictature en place, souvent en pourchassant - sans distinction - criminels de droit commun et opposants politiques, pour des faits réels, soupçonnés, ou totalement imaginaires. Très peu de gens contestent le caractère criminel de régimes tels que le Troisième Reich d'Adolph Hitler, l'Etat Français du Maréchal Pétain ou l'URSS de Joseph Staline. Pourtant les deux premiers sont arrivés aux responsabilités à travers des procédures globalement démocratiques, ce qui montre la difficulté de définir le caractère malfaisant d'un régime par la légalité de son installation au pouvoir. Et si on peut aisément s'accorder sur la dimension démocratique ou dictatoriale de certains régimes, les frontières sont parfois plus floues entre démocratie, autoritarisme et dictature. Comment classer en 2018 des gouvernements comme ceux de Vladimir Poutine en Russie, Recep T. Erdogan en Turquie, ou du Maréchal A-F. al-Sissi Egypte ? A l'évidence la frontière est incertaine, et la confusion est encore plus grande lorsqu'on considère que beaucoup de régimes autoritaires sont le résultat d'une lente dérive de la démocratie vers la dictature. Doit-on alors considérer que les politiques de renseignement menées par ces gouvernements contestables suivraient une pente parallèle à celle de leurs régimes, devant injustes et dangereuses alors qu'elles auraient été justifiées auparavant ? A maintes reprises dans le passé, et encore aujourd'hui, les terroristes d'un jour peuvent être considérés comme les résistants du lendemain pour peu que leurs partisans deviennent représentants de l'ordre légal. Cela signifie-t-il que l'intérêt de la nation a lui aussi changé dans le même temps, ou bien a-t-il toujours été le même ? Est-ce seulement l'interprétation officielle de l'intérêt général qui a changé, ou peut-être n'y a-t-il en fait jamais eu que des intérêts individuels complexes et contradictoires, ne permettant au mieux que de dégager momentanément un intérêt majoritaire ?[18] Sans même devoir apporter de réponse à ces questions, la réalité apparaît tout en nuance : il est illusoire de considérer que l'Etat est fondamentalement respectueux de ses citoyens et bienveillant envers eux. L'Etat ne forme pas un bloc : même si les services de renseignement travaillent avec sérieux et bonne volonté, l'utilisation que les dirigeants décident de faire des renseignements collectés peut toujours varier en fonction des personnes, du contexte. Pour se faire une opinion des limites qu'un système de renseignement doit respecter, chacun peut se demander s'il confierait avec une égale confiance un tel pouvoir de surveillance à tous les partis politiques, extrême-droite et extrême-gauche comprises. Un argument courant consiste à noter qu'un régime authentiquement autoritaire ne se préoccupe nullement des limites légales à son pouvoir de surveillance. On peut certes le penser, mais si nous donnions par avance à un régime aux velléités autoritaires les outils légaux pour opprimer ses citoyens, cela ne trahirait-il pas notre propre acceptation tacite de l'autoritarisme ? En outre, l'existence de contre-pouvoirs, même si elle devait s'avérer inefficace, a au moins le mérite de constituer un dispositif d'alerte capable de signaler l'entrée dans une « zone de danger » juridique et politique.

Au-delà des intentions de l'Etat, se dessine un autre type de risque engendré par la collecte massive de données, celui d'une mise en danger involontaire de ces précieuses ressources personnelles à cause de dispositions de sécurité informatique insuffisantes. En effet, la centralisation d'une telle masse de données est une tentation très forte pour les cyber-pirates de tous calibres, du petit hacker amateur au groupe cyber-criminel professionnel, agissant parfois sur ordre d'une puissance étrangère hostile. C'est officiellement une des raisons qui aurait poussé Apple à refuser les "portes dérobées" demandées par le FBI suite à l'attentat de San Bernardino : la peur de confier les clés à un gardien vulnérable et trop imprudent. L'attaque informatique massive dont la NSA a fait l'objet à l'été 2016 en a apporté la preuve, au cours de laquelle de nombreuses données ont

[18] Serge Schweitzer développe cette idée dans « Un chemin dissident : l'intérêt général ou l'invention d'un faux concept », in Les métamorphoses de l'intérêt général, Presses Universitaires de l'ICES, nov. 2013, pp. 191-207.

été volées par un groupe que certains experts soupçonnent d'être soutenu par l'Etat Russe[19]. Et si on peut admettre que la collecte initiale de données répond à un impératif purement sécuritaire, sans intention de nuire à ceux que l'on surveille, il est en revanche certain que ces mêmes données, lorsqu'elles se retrouvent entre les mains de pirates informatiques motivés par l'appât du gain, deviennent alors un outil de chantage et d'extorsion. Pour exemple de la faillite des autorités à assurer efficacement la sécurité de leurs propres ressources informatiques, on pourra également citer l'affaire des e-mails de l'ancienne Secrétaire d'Etat Hillary Clinton qui a admis avoir échangé des informations sensibles en passant par une messagerie privée non-sécurisée[20], ce qui a permis au site Wikileaks de s'emparer de toute l'archive pour la mettre à disposition d'Internet[21]. En France, la condamnation du blogueur "Bluetouff" (Olivier Laurelli) confirmée en 2015[22] a mis en lumière de graves failles de sécurisation des données dans des agences publiques. Bluetouff avait découvert au hasard d'une recherche Google des documents en principe confidentiels qui étaient librement accessibles sur un serveur mal sécurisé de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES). Le hacker-blogueur avait téléchargé 7,7 Go de données depuis un VPN lui appartenant au Panama, et en avait exploité 250 Mo pour les besoins d'un article sur la légionellose, basé sur les documents obtenus.

Ce risque de mise en danger des données personnelles n'est pourtant pas la principale justification du droit à la vie privée. Les générations précédentes, dans l'histoire politique moderne, ont attaché une importance fondamentale à la liberté de communiquer à l'abri de toute surveillance systématique. Balayer d'un revers de la main leur préoccupations à ce sujet avec pour tout argumentaire "si vous n'avez rien à cacher, vous n'avez rien à craindre" serait faire insulte à leur intelligence. La religion, la sexualité, la santé, les opinions politiques sont des informations à peine moins sensibles aujourd'hui qu'il y a un ou deux siècles, y compris dans les démocraties occidentales dont le statut de démocratie n'est jamais définitivement acquis. Une communication privée peut-elle être véritablement sincère si elle s'effectue avec la conscience de divulguer ces informations dans le présent et dans le futur, à des personnes et institutions que nous ne sommes pas certains d'approuver pour toujours ou d'avoir seulement la possibilité de les approuver ? La comparaison avec les nombreuses informations dont disposent à notre sujet des entreprises privées comme Google ou Facebook est tentante, mais peu pertinente. La collecte d'information par le privé est consentie et éclairée (pour qui prend la peine de lire les conditions générales d'utilisation de ces services), ces informations peuvent d'ailleurs être modifiées ou supprimées, au contraire des informations dont disposent à notre sujet les services de renseignement de l'Etat (le droit de suppression/modification, en revanche, existe pour les informations dont disposent certaines administrations publiques). Ajoutons que les entreprises privées n'ont pas le pouvoir de produire du droit imposable par la violence légale, ce qui relativise la menace de voir nos données utilisées contre nous par ces firmes, sauf si elles-mêmes viennent à partager ces informations avec les autorités publiques, de gré ou de force. Ce dernier cas de figure ne fait que recentrer le raisonnement sur la responsabilité publique, que celle-ci s'exerce directement ou par le truchement d'entreprises privées.

Est-ce à dire que les entreprises privées ne mettent pas en danger nos données, ou les collectent de manière parfaitement transparente ? L'affaire Cambridge Analytica, qui implique une entreprise britannique de collecte et d'exploitation de données dans le cadre de campagnes électorales, ainsi

[19] https://www.bloomberg.com/news/articles/2016-08-17/leak-of-nsa-hacking-tools-raises-questions-of-who-did-it-and-why

[20] http://www.lefigaro.fr/international/2016/10/28/01003-20161028ARTFIG00413-comprendre-l-affaire-des-emails-d-hillary-clinton-en-quatre-points.php

[21] On peut librement effectuer sur le site de Wikileaks des recherches dans cette archive piratée. Il est toutefois à noter que les motivations parfois troubles de Wikileaks dans la divulgation de cette archive a donné lieu à des soupçons de falsification qui doivent nous inviter à la prudence quant au contenu des e-mails. https://wikileaks.org/clinton-emails/

[22] https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000030635061

que le réseau social Facebook, nous permet quelques observations intéressantes. La polémique vient du fait que des données d'utilisateurs auraient été collectées par la ruse, conservées malgré des demandes de suppression puis utilisées pour la campagne électorale victorieuse du Président américain Donald Trump en 2016[23]. On notera que les données concernées ont été récoltées par le biais d'un test de personnalité comme on en trouve beaucoup sur Facebook, et que les utilisateurs remplissent souvent sans trop de précautions. Si la destination finale des données n'apparaissait pas clairement, cela demeure une divulgation volontaire, dont on ne peut même pas dire qu'elle ait été effectuée en échange d'une prestation indispendable. Les conséquences sont par ailleurs importantes pour l'entreprise qui risque de voir ses utilisateurs abandonner l'utilisation du réseau social, notamment à la suite d'appels publics à supprimer Facebook, émanant de personnalités aussi influentes qu'Elon Musk (PDG médiatique de Tesla et Space-X). La capitalisation boursière de Facebook a baissé de près de 50 milliards de dollars dans les jours suivant la révélation de l'affaire par la presse, et le PDG de l'entreprise a personnellement signé une tribune d'excuse largement relayée par une pleine page de publicité payante dans le New-York Times. Il est donc d'une banale évidence de constater que l'impact d'une collecte non consentie ou d'une mauvaise gestion des données est infiniment plus important sur une entreprise privée soumise à la concurrence et dont la survie dépend de ses clients, que sur une agence para-publique en monopole dans son activité, financée par le fruit de l'impôt.

L'état de droit s'applique-t-il aux Etat ?

La voie politique et institutionnelle pour assurer l'existence des libertés individuelles numériques

Dans cette seconde partie, nous allons comparer deux approches possibles dont le but est identique : ramener la finalité et surtout les méthodes du renseignement moderne dans le cadre qui fut longtemps celui des grandes démocraties occidentales, c'est-à-dire la liberté et le secret des correspondances pour tous, et une collecte de données limitée aux personnes déjà soupçonnées d'activités illégales, le tout dans un espace règlementaire strictement défini et en présence de contre-pouvoirs contraignants et réellement aptes à mettre fin aux dérives que nous avons décrit dans la première partie. Nous qualifierons la première approche de légaliste et collective, puisqu'elle consiste à utiliser les outils institutionnels des sociétés démocratiques pour rétablir la situation qui prévalait jusqu'à la fin du 20ème siècle et s'assurer qu'elle cesse de dériver doucement mais sûrement vers une forme d'Etat policier.

Contrairement à une idée répandue, le législateur a prévu des mécanismes légaux pour permettre aux lanceurs d'alerte de dénoncer des dysfonctionnements au sein de l'appareil d'Etat tout en restant dans le cadre de la loi. Aux Etats-Unis Edward Snowden n'a pas été le premier "insider" à dénoncer les pratiques de son employeur. Dans les années 2000 plusieurs agents haut placés, parmi lesquels Thomas Drake et John Crane, ont utilisé les voies légales pour alerter leur hiérarchie sur des agissements qu'ils estimaient manifestement contraires aux lois et procédures auxquelles sont soumises les agences de renseignement. Les agences gouvernementales ne se sont pas contentées d'ignorer leurs alertes : elles ont mis un coup d'arrêt à la carrière des intéressés et multiplié les pressions pour les réduire au silence[24]. C'est d'ailleurs ce double épisode qui aurait décidé

[23] Le Figaro, 23 mars 2018 http://www.lefigaro.fr/secteur/high-tech/2018/03/25/32001-20180325ARTFIG00090-cambridge-analytica-tout-comprendre-sur-une-semaine-de-scandale-pour-facebook.php

[24] Les détails sont donnés par Mark Hertsgaard dans son ouvrage "Bravehearts: Whistle Blowing in the Age of Snowden" (éditions Hot Books), et repris dans le journal américain New-Yorker (23 mai 2011) http://www.newyorker.com/reporting/2011/05/23/110523fa_fact_mayer et dans un article

Snowden, une fois confronté à un choix semblable, à ne pas faire confiance à la procédure légale et à lui préférer une révélation publique pour s'assurer d'un impact médiatique réel[25]. Pourtant le président Barack Obama a publiquement déploré le geste du lanceur d'alerte[26], mettant plus tard en doute ses intentions et dénonçant le recours aux médias plutôt qu'aux procédures légales qui existent dans les agences de renseignement, et par lesquelles les lanceurs d'alerte sont protégés par la loi. Que dit réellement la loi ? Le Washington Post s'est penché sur la question[27], et ses conclusions sont mitigées. Il existe bien une loi datant de 1989 sur la protection des lanceurs d'alerte travaillant pour le gouvernement fédéral, et une loi de la même année visant spécifiquement les services de renseignement.[28] Toutefois sa portée réelle est souvent considérée comme limitée puisque malgré cette législation protectrice une peine d'emprisonnement a été requise contre John Crane, avant que le procureur ne décide de retirer ses accusations de trahison. Le président Obama a lui-même souhaité renforcer cette protection en 2012[29], et a émis dans la foulée une directive à laquelle se réfèrent Edward Snowden et lui-même pour en faire un interprétation contraire. Snowden affirme que la directive PPD-19[30] se limite à protéger les employés des agences de renseignement, mais exclut de son application les prestataires extérieurs travaillant pour le compte des agences comme la NSA, dont il était. En réalité la directive n'exclut pas explicitement les prestataires, mais ne les inclut pas de façon suffisamment claire. Dan Meyer, coordinateur officiel de la PPD-19 dans la communauté américaine du renseignement, l'interprète pour sa part de la façon suivante : les prestataires, sauf indication contraire du gouvernement dans le futur, sont normalement couverts par la section B de la directive censée assurer que toute personne ayant accès à des documents classifiés ne puisse pas s'en voir retirer l'accès. Mais rien n'indique selon lui une protection des prestataires sous la section A, celle qui interdit les mesures de rétorsion à l'égard des lanceurs d'alerte[31]. On peut comprendre qu'une telle ambigüité ait pu dissuader Edward Snowden d'utiliser les voies légales, alors que l'expérience de Thomas Drake et John Crane a montré que même les personnes théoriquement protégées ne sont pas à l'abri de poursuites judiciaires et autres mesures de réprimande dans les faits. Parallèlement au renforcement de la protection pour ceux que l'administration veut bien qualifier de lanceurs d'alerte, le même président Obama a institué une cellule chargée de lutter contre les menaces intérieures aux services de renseignement, la "National Insider Threat Task Force"[32]. Il est donc hasardeux pour un aspirant lanceur d'alerte de passer à l'action, puisque son sort dépend de la vision que les autorités voudront bien avoir de son geste, même lorsque ce geste s'effectue par les voies légales.

---

récent et détaille du quotidien The Guardian (22 mai 2016) https://www.theguardian.com/us-news/2016/may/22/how-pentagon-punished-nsa-whistleblowers

[25] AJ+ dans Medium, 25 août 2015 https://medium.com/@ajplus/exclusive-edward-snowden-interview-about-fellow-nsa-whistleblower-thomas-drake-7b0d1dce270

[26] On se reportera entre autres à cette conférence de presse du Président Obama (à partir de 01:20) https://www.youtube.com/watch?v=tysIV6t54L4

[27] Glenn Kessler dans le Washington Post, 12 mars 2014https://www.washingtonpost.com/news/fact-checker/wp/2014/03/12/edward-snowdens-claim-that-as-a-contractor-he-had-no-proper-channels-for-protection-as-a-whistleblower/

[28] "Intelligence Community Whistleblower Protection Act" (loi sur protection des lanceurs d'alerte dans la communauté du renseignement), une législation de 1989.

[29] Whistleblower Protection Enhancement Act (loi sur le renforcement de la protection des lanceurs d'alerte), révision en 2012 de la loi de 1989 citée supra.

[30] Presidential Policy Directive 19, consultable en ligne : http://www.fas.org/irp/offdocs/ppd/ppd-19.pdf

[31] Dan Meyer propose cette interprétation dans une conférence du 25 février 2014 à l'Université de Georgetown, dont la vidéo est accessible en ligne http://www.law.georgetown.edu/academics/centers-institutes/national-security/Events/Past-Events.cfm

[32] Executive Order 13587, consultable en ligne : https://www.ncsc.gov/publications/policy/docs/EO_13587.pdf. Le groupe de travail "National Insider Threat Task Force" dispose également d'une vitrine sur le web https://www.ncsc.gov/nittf/

Un des problèmes auxquels on se heurte en voulant réformer le système dans les formes démocratiques est la capacité des services de renseignement à couvrir leurs actions par des obligations de silence imposées à leurs interlocuteurs. Aux Etats-Unis cela prend la forme des "gag orders", c'est-à-dire des "baillons" imposés à des interlocuteurs des services de renseignement pour les empêcher légalement de révéler à quiconque les demandes qui ont pu leur être faîtes par les renseignements américains. Cet outil dont l'esprit était de ne pas alerter les cibles de la surveillance dont elles pouvaient faire l'objet, a toutefois un défaut important : il peut à tout moment devenir abusif lorsqu'il est utilisé pour couvrir une demande non-conforme aux principes qui régissent le renseignement, ne laissant alors aucune possibilité au public ou à la presse d'accéder légalement à l'information selon laquelle les services de renseignement s'aventurent au-delà des limites légales de leur champ d'action. Les grands acteurs du numérique, en particulier dans la Silicon Valley, se sont souvent montrés inquiets face à l'existence de ces "gag orders", craignant de perdre la confiance de leurs clients dans la sécurité et la confidentialité de leurs données. C'est ainsi qu'une entreprise comme Apple a trouvé un moyen détourné de contourner le principe du baillon légal en mentionnant systématiquement dans son rapport annuel qu'elle n'avait pas fait l'objet de demandes particulières des services de renseignement au titre de la section 215 du Patriot Act[33]. Naturellement lorsque cette mention a été sensiblement modifée dans le courant de l'année 2013, la presse a spéculé sur les requêtes des services de renseignement américains accompagnées de baillons légaux, même si personne n'a pu déterminer avec suffisamment de certitude la nature et le nombre exact de ces requêtes, notamment en raison de la complexité des mécanismes légaux qui régissent ces procédures.

En France la voie légale est en train de devenir singulièrement moins efficace depuis le vote de la loi sur le renseignement en 2015. Cette dernière a entériné le remplacement de la CNCSI par le CNCTR pour faire office d'organisme de contrôle face aux services de renseignement. Comme nous l'avons vu dans la partie précédente, nombreux sont les experts qui estiment que désormais le CNCTR n'aura plus les moyens concrets de vérifier par lui-même dans quelle mesure la surveillance se situe dans le cadre légal ou s'aventure au-delà des limites fixées par le législateur. Le contre-pouvoir semble bien devenir peu à peu inopérant au gré des réformes successives et de l'intensification de la menace terroriste. Peut-on espérer un retour prochain à une demande démocratique de modération dans les pratiques du renseignement ? Cela est peu vraisemblable dans les conditions actuelles. En 2014 - avant le traumatisme des attaques terroristes massives de 2015-2016 - on apprenait par un sondage que la surveillance généralisée des échanges sur Internet, même si elle nuit « gravement » aux libertés individuelles, était « justifiée » pour 57 % des Français à des fins de lutte contre les organisations criminelles, selon le baromètre réalisé par Polling Vox[34]. C'est donc sans surprise qu'en avril 2015, après le massacre de la rédaction de Charlie Hebdo et de l'Hyper Cacher, mais avant le bilan autrement plus lourd des attentats du Bataclan, les Français étaient alors 63% à se déclarer favorables à la limitation des libertés individuelles sur Internet, tandis que deux tiers étaient favorables au dispositif automatique de surveillance des données de navigation des internautes.[35] Une autre étude effectuée au niveau mondial seulement une semaine après les attentats du Bataclan en novembre 2015 est tout aussi éclairante. On y apprend que 71% des Français sont favorables ou très favorables à l'autorisation pour les services de renseignement d'accéder au contenu des communications de leurs citoyens pour des motifs de

[33] Cette pratique est surnommée « warrant canary » par les anglo-saxons, en référence à la présence historique de canaries dans les mines de charbon pour avertir de la raréfaction d'air respirable avant qu'il ne soit trop tard. Des experts en cyber-sécurité comme Bruce Schneier doutent cependant de l'efficacité du warrant canary, estimant qu'un gag order pourrait bien inclure une interdiction d'utiliser ce moyen détourné contraire à l'esprit même du gag order.

[34] Le Monde, 25 février 2014 http://www.lemonde.fr/technologies/article/2014/02/25/la-surveillance-d-internet-justifiee-pour-une-majorite-de-francais_4372732_651865.html

[35] Les Echos, 13 avril 2015 http://www.lesechos.fr/13/04/2015/lesechos.fr/0212267457_projet-de-loi-renseignement---63--des-francais-pour-une-limitation-des-libertes.htm

sécurité nationale[36]. Cette opinion s'exprime en toute conscience, puisque dans le même temps 81% des Français jugent « possible » ou « très probable » que leurs activités en ligne soient censurées ou surveillées – près de 20 points de plus que la moyenne mondiale. Ce penchant des Français pour la sécurité au détriment de la liberté se retrouve sans surprise dans l'offre politique actuelle. La Loi Renseignement, qui marque un tournant historique dans la limitation de la vie privée sous la V^{ème} République, est l'oeuvre d'un gouvernement socialiste, ce qui est très significatif lorsqu'on songe que traditionnellement la gauche française est plus réticente que la droite et l'extrême-droite aux lois sécuritaires. On ne sera pas surpris non plus de constater que les seules forces politiques se disant réticentes aux lois sécuritaires sont situées à gauche du gouvernement et à l'extrême-gauche, soit des courants aujourd'hui largement minoritaires dans le paysage politique français. Tout indique donc que la démocratie française - mais c'est assez largement le cas dans le reste du monde - ne peut aboutir dans le contexte actuel qu'à une surveillance accrue de la part des autorités publiques. De façon paradoxale les Français sont nettement plus inquiets en raison de la collecte de données par des entreprises privées telles que Google ou Facebook, et sont 80% à estimer que le gouvernement n'agit pas suffisamment pour protéger leurs données collectées de cette manière. Une différence de taille mériterait pourtant d'être soulignée plus souvent : la collecte de données par des organisations privées peut être refusée individuellement et un contrat explicite est passé entre l'utilisateur de services comme Google pour l'informer de la nature des données récoltées et de l'utilisation qui en est faite, avec la possibilité à tout moment de cesser le recours à ces services et d'effacer les données précédemment récoltées. L'Etat, quant à lui, impose collectivement ses méthodes et ses finalités de sorte que 51% des citoyens peuvent décider de la limite de la vie privée des 49% restants, sans information claire des quantités de données collectées et de leur utilisation, ni aucune possibilité d'en exiger la destruction immédiate, les délais de conservation ayant au contraire tendance à s'étendre.

Indéniablement la voie légale présente un avantage moral, et on ne pourrait que se satisfaire de parvenir à préserver les libertés individuelles à l'ère du numérique en respectant à la lettre les procédures définies démocratiquement par le peuple souverain. Mais les limites de l'exercice apparaissent bien vite, comme le démontre l'exemple américain. D'autre part, la volonté de respecter les règles institutionnelles démocratiquement établies présuppose implicitement que de son côté, l'autorité publique respecte parfaitement les règles auxquelles elle est soumise. Or, si la tentation existe de contourner la loi du côté des lanceurs d'alerte c'est précisément parce que ces derniers découvrent souvent que l'Etat agit parfois hors de tout cadre légal, et que cette situation n'est pas si exceptionnelle qu'on pourrait l'espérer. Or il existe un déséquilibre intrinsèque entre le citoyen et son Etat, puisque ce dernier possède le monopole de la violence légale et se trouve en situation de réprimer le premier. De ce fait on ne peut pas mettre sur le même plan les agissements hors-la-loi d'un citoyen désarmé physiquement comme symboliquement, et les agissements hors-la-loi d'un Etat qui dispose des moyens militaires et légaux pour s'imposer face à toute tentative de résistance, si légitime qu'elle puisse être parfois. Ceci posé, il nous semble que même en admettant le caractère illégal des révélations d'un lanceur d'alerte comme Edward Snowden, l'opinion devrait s'inquiéter beaucoup plus du contenu des révélations, soit le mépris affiché par certains services de renseignement pour les limites légales censées les encadrer, et l'utilisation de méthodes de surveillance indignes d'une démocratie moderne à des fins outrepassant largement la défense nationale ou la sécurité intérieure. La volonté de combattre l'abus de pouvoir par les outils du droit est moralement louable mais n'en reste pas moins dérisoire en termes d'efficacité en face d'une institution écrasante de supériorité dans tous les domaines.

On peut enfin relever une forme de contradiction entre le caractère fondamentalement individuel de la liberté communiquer librement sans être surveillé (sauf lorsque les autorités ont de bonnes raisons de soupçonner des activités gravement illégales justifiant une surveillance ciblée et limitée dans le temps), et le caractère fondamentalement collectif et majoritaire du fonctionnement des

[36] Centre for International Governance Innovation & IPSOS, https://www.cigionline.org/internet-survey-2016

institutions capables de décider du périmètre de la surveillance et des modalités plus ou moins strictes visant à contrôler son application. Nous avons vu plus haut qu'il est possible, tant dans les faits que dans le droit, de voir disparaître peu à peu le principe du secret des correspondances applicable par défaut à tous les citoyens. Les révélations de Snowden ont montré que la capacité technique existe, les réformes du renseignement qui se succèdent tendent de fait à affaiblir ce principe, et l'opinion publique valide majoritairement ce virage législatif. La question suivante est par conséquent au coeur du problème : est-il acceptable de voir s'affaiblir ou disparaître une liberté par essence individuelle, et même constitutionnelle dans certains pays, sous la pression d'une préférence collective ? La réponse à cette question dépend en grande partie de la conception que nous avons de nos libertés fondamentales, comme celle de communiquer librement à l'abri de la surveillance. Si l'on considère que cette liberté nous est accordée par l'Etat, lui-même rendu légitime par la volonté du peuple, alors il n'est pas inconcevable d'y renoncer tôt ou tard par une décision majoritaire, puisque l'Etat est lui-même issu d'une volonté majoritaire qui s'impose à l'ensemble des citoyens d'une nation sur un territoire donné. Cette conception, pour acceptable qu'elle soit, n'en traduit pas moins la négation du caractère naturel et inné de certaines libertés, dont celle de communiquer librement. L'autre réponse possible nous est donnée par la tradition philosophique libérale, selon laquelle les droits naturels préexistent à l'Etat, dont le rôle se borne à garantir les conditions nécessaires à l'exercice de ces droits. Tant que l'Etat fait consensus dans la manière dont il respecte les droits individuels, alors la question de l'origine de ces droits demeure secondaire. Mais dès lors que l'Etat empiète sur les droits et libertés qu'il est censé garantir, sa légitimité à agir ainsi n'est reconnue que par ceux des individus qui pensent que leur liberté ne préexiste pas à l'Etat. Les autres, ceux qui ne reconnaissent à aucune organisation, démocratique ou non, le droit de les priver d'une liberté naturelle, sont alors confrontés à un dilemme : accepter la nouvelle donne et rester dans la légalité, ou choisir de placer leur droit naturel au-dessus du droit positif et accepter l'idée selon laquelle la moralité se trouve parfois du côté de l'illégalité, le droit pouvant parfois donner une apparence de légitimité à une injustice, pour peu que la majorité y consente.

Contre les dérives de la surveillance, la riposte individuelle extra-légale

La réticence à être surveillé, même sous des motifs de sécurité nationale, ne date certes pas de l'affaire Edward Snowden, mais ce dernier a entraîné un vif débat sur la surveillance étatique, au terme duquel certains sont arrivés à la conclusion que la morale se trouvait désormais hors du droit, parfois même contre le droit. Loin de s'en tenir à une pétition de principe, les partisans de cette option ont beaucoup travaillé dans deux directions complémentaires : d'une part les techniques d'anonymisation pour tout individu ou organisation souhaitant échapper à la surveillance des services de renseignement, et d'autre part une riposte plus active visant à faire subir à l'Etat et dans une certaine mesure aux entreprises la surveillance à laquelle les citoyens sont déjà soumis.

Les révélations d'Edward Snowden, quel que soit le crédit qu'on veut bien leur accorder, ont de fait accéléré une course entre les moyens de communications de plus en plus anonymes et sécurisés pour contourner la collecte de données, et les contre-mesures des services de renseignement qui travaillent constamment à rendre inopérants ces différents systèmes de contournement. C'est une véritable course de l'obus contre la cuirasse numérique, dans laquelle aucun vainqueur clair ne semble se dégager à l'heure où nous écrivons. Entre 2013 et 2018 on a vu se développer un véritable écosystème numérique autour des technologies de communication reposant sur le chiffrement et la cryptographie, ce qui traduit une attente de la part d'une partie du public. Il est aujourd'hui de plus en plus facile de recourir à des outils d'anonymisation pour parcourir le web, comme les différents logiciels issus du projet Tor[37]. Développé pour ordinateurs et périphériques mobiles, le navigateur Tor Browser parvient à brouiller les pistes numériques laissées par un internaute,

[37] http://www.torproject.org

dont l'ordinateur apparaît avec une adresse IP différente de son IP réelle, généralement en provenance d'un autre pays que le sien. C'est précisément ce logiciel qui est utilisé pour accéder au web caché, qui comprend à la fois le Deepweb et le Darkweb, non référencé par les moteurs de recherche et inaccessible aux navigateurs traditionnels tels que Chrome, Firefox, ou Safari. Réputé héberger essentiellement des activités illégales comme la pornographie pédophile, la propagande terroriste et surtout le trafic de drogue, une étude parue à l'automne 2016 montre au contraire que la majorité du web caché ne semble pas abriter d'activités répréhensibles par la loi[38] et qu'en réalité beaucoup d'internautes souhaitent protéger leurs activités en ligne de la collecte de données officielle ou officieuse, ou encore soutenir les opposants politiques dans les pays dictatoriaux qui ont un réel besoin d'anonymat. La solidité de l'anonymat fourni par Tor dépend en grande partie du nombre d'utilisateurs du réseau, ce qui peut pousser des citoyens de démocraties libérales à l'utiliser pour mieux préserver l'anonymat de ceux qui ont un besoin critique de cet anonymat sous peine de lourdes représailles. Mis à part le web, Internet sert aussi à faire transiter des communications entre individus par le biais d'e-mails et de sms, d'où le développement de solutions chiffrées garantissant l'anonymat, parmi lesquelles ProtonMail, un client de messagerie électronique basé en Suisse et entièrement chiffré à l'aide d'un code que l'utilisateur est seul à posséder, rendant extrêmement difficile la saisie de données par des autorités légales même lorsque ces dernières disposent des mandats nécessaires. Pour remplacer les SMS, et puisque la majorité des smartphones dispose d'un accès à Internet, des applications de messagerie chiffrées telles que Signal et Telegram ont vu le jour après 2013. Signal a fait l'objet d'une promotion par Edward Snowden en personne, et a annoncé de nouveaux financements de 50 millions de dollars en 2018 pour son développement[39]. On trouve également Tails, un système d'exploitation complet, qui se transporte sur clé USB et fonctionne sans besoin d'être installé, et dont le fonctionnement est entièrement pensé pour respecter la vie privée et contourner toute forme de surveillance ou de censure. Conscientes de cette attente d'une partie du marché, plusieurs entreprises importantes de l'économie numérique ont misé sur plus d'anonymat et affiché leur réticence à collaborer de manière systématique avec les autorités pour partager les données de leurs utilisateurs. Au-delà du cas très médiatisé d'Apple, qui a décidé de chiffrer par défaut tous les iPhones et de s'en couper volontairement l'accès pour ne pas être forcé de collaborer avec les autorités[40], on relève une décision similaire chez WhatsApp, l'application de messagerie la plus populaire au monde (plus d'un milliard d'utilisateurs), qui a instauré le chiffrement par défaut pour tous les échanges de messages[41]. Au-delà des communications, la préoccupation de l'anonymat et la défiance vis-à-vis de l'Etat est omniprésente dans la communauté grandissante des utilisateurs de crypto-monnaies telles que Bitcoin. Celle-ci est-elle la monnaie des terroristes qu'ont voulu décrire certains médias et politiques ? Il est extrêmement difficile d'y apporter une réponse car les études se contredisent, et que l'usage de Bitcoin dans le domaine légal varie considérablement au gré de la législation encore incertaine et instable, des frais de transaction parfois élevés, autant d'inconvénients qui n'en sont pas pour les délinquants utilisateurs de cette monnaie. La philosophie de Bitcoin rejoint largement celle des autres outils d'anonymisation puisqu'elle met l'accent sur la liberté de ne pas subir la surveillance de nos transactions par l'Etat et de ne pas être victimes d'une politique monétaire centrale inflationniste. Les utilisateurs de Bitcoin, de Tor, de Signal et de la vaste galaxie d'outils d'anonymisation en ligne ont pour une large partie d'entre eux renoncé à faire valoir leurs opinions sur le marché politique démocratique, et ont fait le choix de "hacker" l'Etat, c'est-à-dire d'opérer en parallèle de la loi (c'est le cas de Bitcoin, qui à ce jour ne fait pas l'objet d'une législation

[38] Source : étude Terbium Labs, firme spécialisée dans la sécurité des données, en particulier sur le web caché. L'étude porte sur un échantillon de sites web cachés que Terbium a voulu représentatifs, mais il était impossible de mener une étude quantitative rigoureuse portant sur l'ensemble du web caché, ce dernier étant par définition non-indexé.

[39] Newsweek, 22 février 2018 http://www.newsweek.com/bad-news-fbi-edward-snowdens-favorite-chat-app-signal-just-got-50m-funding-816035

[40] The Guardian, 17 octobre 2014 https://www.theguardian.com/technology/2014/oct/17/apple-defies-fbi-encryption-mac-osx

[41] https://www.whatsapp.com/faq/en/general/28030015

claire en France et dans de nombreux pays) et de ne pas hésiter à aller contre elle s'ils estiment injustifiées le lois qui régissent leur navigation et leurs communications en ligne. Cette approche est plus difficile à défendre en démocratie, notamment en raison du caractère ambivalent des outils utilisés par d'honnêtes citoyens soucieux de leur vie privée et qui bénéficient dans le même temps aux terroristes de toutes sortes. Mais les adeptes de cette approchent n'ont vraisemblablement pas comme préoccupation première d'avoir la reconnaissance ou la considération du reste de la société, tant que leurs outils fonctionnent et permettent de contourner l'Etat.

Malgré l'efficacité apparente des outils d'anonymisation, l'Etat consacre des moyens humains et financiers croissants à la mise au point de contre-mesures encore plus efficaces, des "obus numériques" capables de percer cette "cuirasse de chiffrement" toujours plus épaisse. Ainsi les experts s'accordent à reconnaître que le réseau Tor n'est pas une garantie absolue d'anonymat et que ses utilisateurs peuvent être démasqués individuellement lorsque les services de renseignement y consacrent des moyens suffisants[42]. En France, un homme a fait l'objet d'une condamnation à de la prison ferme[43] pour avoir incité un autre à des actions terroristes dans divers messages envoyés avec Telegram, une application de messagerie normalement privée et sécurisée. Il est pourtant possible par divers moyens d'infiltrer les réseaux terroristes sur Telegram, même lorsque ces derniers prennent un maximum de précautions pour respecter le chiffrement de leurs communications[44]. On peut y voir l'illustration d'un nouvel équilibre trouvé, bien involontairement, entre liberté et sécurité. A travers l'utilisation croissante du chiffrement par des utilisateurs honnêtes en plus des vrais terroristes, la collecte "au chalut" de données de communication est rendue plus difficile, incomplète, et vraisemblablement inefficace. Cela n'empêche pas les enquêtes ciblées, et à ce jour les experts en sécurité informatique sont globalement d'accord pour reconnaître qu'avec suffisamment de moyens techniques et humains, aucun protocole de communication n'est capable d'assurer un anonymat total dans le présent comme dans le futur. Autrement dit, même un chiffrement résistant aux services aujourd'hui pourra tomber sous les coups de boutoir informatiques des super-ordinateurs de demain.

Nous voilà donc revenus au point de départ : le secret des correspondances comme règle générale (sous réserve de quelques manipulations accessibles à l'utilisateur moyen) et la possibilité de briser cet anonymat dans les cas où l'on considère que le risque pour la sécurité nationale justifie l'allocation de moyens importants. A ceci près que ce retour au point de départ n'existe que dans les faits, mais nullement en droit, où la collecte de données en masse est en train de devenir la règle. Cette situation correspond bien à ce que nous savons de la pensée d'Edward Snowden lorsque ce dernier a fait ses révélations. L'ex-prestataire de la NSA n'est pas fondamentalement hostile au principe du renseignement dans lequel il a fait toute sa carrière, ni à la légitimité de l'Etat à assurer la sécurité intérieure et extérieure (il est issu d'une famille de tendance conservatrice et patriote, largement favorable à l'Etat). Le détail de la méthode employée pour ses révélations de juin 2013 est riche d'enseignements. Snowden a toujours refusé de divulguer lui-même les documents qu'il détenait, et n'a pas non plus envoyé ces documents à l'ensemble de la presse du monde entier. Au contraire il a établi des liens de confiance avec une poignée de journalistes d'investigation réputés pour leur sérieux, et ne leur a posé comme seules conditions qu'un engagement à faire connaître au public la situation de la surveillance, et de prendre un soin particulier à ne rien dévoiler qui risquerait de mettre en danger des personnes ou des nations. Dans le docu-

[42] Circuit Fingerprinting Attacks: Passive Deanonymization of Tor Hidden Services. Albert Kwon, Mashael AlSabah, David Lazar, Marc Dacier, et Srinivas Devadas. Massachusetts Institute of Technology, Université du Qatar et Qatar Computing Research Institute. http://people.csail.mit.edu/devadas/pubs/circuit_finger.pdf

[43] Le Monde, 30 septembre 2016 http://www.lemonde.fr/police-justice/article/2016/09/30/un-homme-condamne-a-deux-ans-de-prison-ferme-pour-incitation-au-terrorisme-sur-telegram_5006459_1653578.html

[44] France TV Info, 11 août 2016 http://www.francetvinfo.fr/monde/terrorisme-djihadistes/cinq-moyens-d-enqueter-sur-telegram-lamessagerie-des-jihadistes_1584435.html

mentaire Citizen Four, on voit même Snowden se couper toute possibilité d'accès aux documents au moment de les confier à ses partenaires journalistes, en leur témoignant explicitement sa totale confiance dans leur capacité à gérer ces délicates révélations de la manière la plus responsable possible. Si on s'en tient à son discours et ses actions connues, Snowden ne cherche pas à saper les services de renseignement en tant que tels, mais à créer un choc d'opinion pour les forcer à revenir dans les limites légales.

On a souvent comparé Edward Snowden à un autre célèbre lanceur d'alerte, hacker et militant pour la liberté des communications numériques individuelles : Julian Assange (voir encadré). Le fondateur et principale tête pensante de Wikileaks (unique, à en croire de nombreux témoignages) a effectivement des liens avérés avec Edward Snowden, puisque c'est Wikileaks qui a notamment contribué à assister Snowden dans sa fuite devant les représailles américaines[45], même si on ne leur connaît aucun lien particulier avant le coup de tonnerre médiatique des révélations de juin 2013. A première vue le parallèle semble donc pertinent, mais à mieux y regarder Julian Assange représente un courant plus radical dans la contestation du pouvoir de l'Etat. On ne sera pas surpris de constater que Wikileaks milite activement contre toute forme de surveillance des communications, mais la philosophie qui anime l'organisation est nettement plus offensive et ne se limite pas à la problématique de la surveillance. Elle inverse totalement la problématique, et ne se contente pas de nier le droit de l'Etat à surveiller ses citoyens, mais revendique le droit pour les citoyens à surveiller leur Etat, ainsi que toute autre organisation publique ou privée qui détient une forme de pouvoir politique ou économique. Wikileaks prend donc le contre-pied total des gouvernements qui réclament plus de lois sécuritaires, et double cette critique d'une accusation sous-jacente d'abus de pouvoir et de mensonge en direction des citoyens. Cette radicalité philosophique se retrouve dans les méthodes : Wikileaks révèle des documents sans filtre, souvent sans intermédiaire, et d'après des journalistes reconnus qui ont travaillé avec lui sur la révélation des 250.000 câbles diplomatiques, Julian Assange assume son choix de ne pas masquer dans les documents les informations pouvant mettre en danger des personnes, en l'occurence les informateurs locaux qui travaillaient avec les ambassades américaines à l'étranger. Assange trouve normal d'appliquer sa propre radicalité à des personnes dont la situation est pourtant complexe, estimant que chacun doit porter la responsabilité de ses actes et que rien ne justifie que l'on cache une vérité, pas même la mise en danger d'individus[46]. Pour ajouter à sa réputation sulfureuse, Julian Assange entretient des liens avec la Russie de Vladimir Poutine que la Maison Blanche et le Département d'Etat ne cessent de condamner comme une collaboration coupable avec celui qui apparaît de plus en plus clairement comme un ennemi de l'Etat américain. Il est vrai que Julian Assange a toujours fait des Etats-Unis sa cible favorite, il est aussi vrai que des médias russes presque toujours alignés sur les positions du Kremlin ouvrent autant que possible leurs colonnes et leurs micros au fondateur de Wikileaks, qui depuis son refuge de l'ambassade d'Equateur à Londres intervient régulièrement dans des médias à la réputation douteuse, tant que ces derniers sont prêts à lui accorder une tribune. Les derniers mois de la campagne présidentielle américaine pour les élections de novembre 2016 ont été marqués par la révélation publique par Wikileaks de documents considérés comme compromettants pour la candidate démocrate Hillary Clinton, ce qui a valu à Wikileaks une accusation de favoritisme pour Donald Trump. Si Assange n'a jamais exprimé de sympathie pour Donald Trump et que ce dernier n'a jamais caché son hostilité aux lanceurs

[45] Sarah Harrisson, autre figure connue de Wikileaks, a personnellement accompagné Snowden dans sa longue rétention administrative à l'aéroport de Moscou avant de se voir accorder l'asile politique par la Russie.

[46] A ce jour personne n'a pu relier la révélation des câbles diplomatiques à la mort ou la torture d'informateurs pour les ambassades américaines, mais tout porte à croire que certains de ces informateurs ont dû fuir des représailles de dirigeants locaux lorsque leur nom est apparu dans les câbles.

d'alerte autoproclamés[47], il est certain en revanche qu'il existe un conflit personnel entre Hillary Clinton et Julian Assange, la candidate démocrate étant chargée en tant que Secrétaire d'Etat en 2010 de riposter à l'affaire des câbles diplomatiques et des War Logs, déclenchant le blocus financier contre Wikileaks et la traque sans relâche de son dirigeant. Il est également certain que la mauvaise publicité qui est faite aux Etats-Unis et à d'autres démocraties occidentales ciblées par Wikileaks permet à Moscou de relativiser ses propres manquements à la démocratie, ainsi que de se poser en protecteur des dissidents pourchassés par ces mêmes démocraties en leur accordant l'asile politique. Rien ne permet toutefois d'affirmer que la diplomatie russe pilote directement Wikileaks, tout au plus peut-on soupçonner des groupes de hackers russes de se charger de certains vols de documents pour les fournir à Wikileaks, les premiers hackers choisissant soigneusement leurs cibles afin de fournir aux seconds des documents conformes aux objectifs géopolitiques de leurs commanditaires présumés.

L'organisation Wikileaks a donc des méthodes contestées, et son principal dirigeant est une personnalité extrêmement controversée, y compris dans son propre camp[48]. Mais même en admettant un biais dans le choix des documents révélés, on ne peut pas se contenter de détourner le regard des documents fournis par l'organisation. D'abord l'authenticité des documents est très rarement remise en cause par les intéressés, et par ailleurs ils montrent un niveau de malhonnêteté inquiétant à haut niveau dans l'appareil d'Etat. L'observateur averti de la vie politique et de l'exercice du pouvoir pourra ironiser à propos de l'étonnement du public en apprenant que l'appareil diplomatique est utilisé à des fins d'espionnage économique, que les diplomates cherchent les pires secrets chez leurs interlocuteurs afin de disposer de leviers d'action efficaces au moment opportun. Ou encore que l'armée américaine a torturé à Guantanamo et commis des crimes de guerre en Irak. Depuis Machiavel et même avant lui, nous savons que dans les faits si ce n'est dans le droit, pour un Etat, la fin justifie les moyens. Dans un ouvrage paru en 2015, Geoffroy de Lagasnerie tente une défense des lanceurs d'alerte centrée sur les personnes de Julian Assange, Bradley/Chelsea Manning, et Edward Snowden. A la suite de Judith Butler[49], il y relève une tendance inquiétante de l'Etat à affirmer sa souveraineté, sa supériorité au reste de la société en recourant au "hors-droit", par exemple avec les assassinats ciblés par drones, ou encore la rétention administrative indéfinie et sans procès ni inculpation pour les prisonniers de Guantanamo. Le hors-droit n'est plus un un « à-côté » qui attendrait d'être régulé ou un « avant-droit » qui aurait perduré, il est délibéré. Dans ces conditions le déséquilibre gouvernant/gouverné est accru, et la contestation par des moyens a-légaux voire illégaux ne serait qu'une réponse proportionnée à la manière dont le gardien du droit s'affranchit de ses propres règles[50].

Geoffroy de Lagasnerie propose une vision nouvelle de l'option que nous avons décrite précédemment, soit la volonté de "hacker" l'Etat. Il tient en particulier à la différencier de la désobéissance civile, un concept souvent invoqué pour décrire les motivations de Julian Assange ou Edward Snowden. Elle n'a de sens que dans une démocratie, et même si elle est le fait d'une minorité elle se fait au nom de la majorité, au nom des valeurs communes de l'état de droit et de la justice. Elle est publique, souvent même avec préavis raisonnable. Ce n'est paradoxalement pas un défi à l'Etat, mais une tentative de le ménager, de le réformer, les dissidents se veulent plus légalistes que l'Etat. Il ne cherchent surtout pas à fuir la punition, elle est une étape importante du pro-

[47] Dans une interview accordée à Fox News en 2013, celui qui n'était pas encore candidat à la présidentielle américaine s'était prononcé pour la liquidation physique des personnes comme Snowden ou Assange. https://www.youtube.com/watch?v=T4DjrBC4K-Q

[48] Edward Snowden, que Wikileaks avait aidé dans sa fuite en 2013, a publiquement critiqué en 2016 le refus catégorique de l'organisation "d'éditer raisonnablement" les documents qu'elle publie, ce qui lui a valu une réponse acerbe de Wikileaks l'accusant d'opportunisme en vue d'une grâce présidentielle.

[49] Judith Butler : "Vers la cohabitation" (Paris, Fayard, 2013)

[50] Geoffroy de Lagasnerie : "L'art de la révolte : Snowden, Assange, Manning" (Paris, Fayard, 2015)

cessus. Snowden et Assange entrent plus difficilement dans un tel schéma, au sens où ils se sont affirmés publiquement, mais ont aussi assuré leur fuite autant que possible, et ainsi questionné notre rapport à l'Etat, aux frontières, à la nation. Chez Jean-Jacques Rousseau ou chez John Rawls[51] on réfléchit sur le contrat social et les modes de co-existence en tenant pour acquis sans le questionner le fait que nous sommes dans un état de fait qui nous force à coexister dans des entités déjà définies et qu'on ne peut modifier. La plupart des modes de révolte ont pour conséquence de ratifier de fait l'appartenance à la communauté que l'on n'a pas choisie. Tandis que la fuite questionne cet état de fait, politise enfin la question de l'appartenance à un Etat. Snowden et Assange refusent de se soumettre à une justice qu'ils ne considèrent pas comme la leur ou dont ils contestent l'impartialité. Ils vont à l'encontre du classique « je fais confiance à la justice de mon pays », ils s'en éloignent au maximum. Il ne faut donc pas parler de désobéissance civile pour Snowden, qui choisit volontairement de ne pas jouer selon les règles de sa communauté. Les actions de Snowden ou Assange ne sont pas une tentative de faire perdurer une ancienne coutume contre un nouvel ordre juridique en cours d'installation, mais plutôt une volonté d'inventer quelque chose de nouveau. La contestation politique telle que définie auparavant est limitée dans sa radicalité par l'obligation d'entrer dans un dialogue, une acceptation de la négociation, une reconnaissance des limites du conflit avant même d'entrer dans le conflit. L'anonymat libère les individus de cette obligation de soumission à celui qu'on considère comme oppresseur. Il remet en cause l'analyse Hegelienne de la politique comme recherche implicite de reconnaissance et de volonté de construction d'un cadre communicationnel.

Nous souscrivons volontiers à cette analyse dans le cas de Julian Assange, tandis que le cas Snowden est un peu plus complexe. Il semble toutefois que si dans un premier temps la démarche d'Edward Snowden pouvait tenir dans une certaine mesure de la désobéissance civile, la violence de la réaction du pouvoir américain a poussé le lanceur d'alerte dans une forme de radicalité plus volontiers assumée, c'est du moins ce qui apparaît de ses nombreuses prises de paroles et autres expressions publiques depuis sa résidence moscovite, notamment sur Twitter.

Conclusion :

A moins de se projeter dans une nouvelle forme d'organisation politique foncièrement différente des Etat-nations contrôlant un territoire donné et tous les citoyens soumis à sa nationalité, il n'est probablement pas raisonnable ni réaliste de vouloir une opacité totale et absolue des communications inter-personnelles et autres aspects de la vie privée, tandis que l'Etat serait soumis à une transparence totale, permanente et immédiate. On peut néanmoins considérer comme dangereux à long terme d'inscrire dans le droit le principe d'une surveillance généralisée, fût-ce au nom d'une plus grande sécurité. Le caractère démocratique d'un Etat n'est en aucun cas assuré de persister dans le futur. Renoncer à sa vie privée, même lorsqu'on n'a rien à cacher, revient à s'affaiblir d'avance, à se priver de son principal outil de résistance dans l'éventualité d'une dérive totalitaire du même type que celles du 20ème siècle. La conservation des données collectées en masse ouvre par exemple la porte à une exploitation rétro-active des données collectées en un moment donné. Qu'il nous suffise d'imaginer ce que les nazis ou les soviétiques auraient pu faire des montagnes de méta-données dont nos Etats modernes disposent aujourd'hui. Ne rien avoir à cacher dans le présent ne prémunit en rien d'une oppression future, sur une base factuelle pourtant inchangée. Etant donné ce risque, il nous semble souhaitable de revenir au minimum à la situation d'avant le 11 septembre 2001, où la surveillance était beaucoup plus ciblée et mieux encadrée. Pour y arriver, la voie légale est une option louable, voire prioritaire, mais elle apparaît insuffisante pour atteindre son objectif. Dans la mesure où elle permet de faire respecter un droit naturel, ou de dénoncer les agissements illégaux des gouvernants, la voie extra-légale et parfois même illégale pourrait bien s'avérer salutaire, ce serait loin d'être la première fois dans notre histoire.

Pierre Schweitzer

[51] John Rawls développe cette idée dans "Théorie de la justice" (Paris, Seuil, 1987)

Bibliographie

ASSANGE J. (dir), *Menace sur nos libertés*, Robert Laffont, 2013.
ASSANGE J., *Google contre Wikileaks*, Ring, 2018.
BUTLER J., *Vers la cohabitation*, Fayard, 2013.
DE LAGASNERIE G*., L'art de la révolte : Snowden, Assange, Manning*, Fayard, 2015.
GREENWALD G., *Nulle part où se cacher*, JC Lattès, 2014.
GUERRIER C., *Les enjeux de la société de contrôle à l'ère du numérique*, ISTE, 2017.
HERTSGAARD M., *Bravehearts: Whistle-Blowing in the Age of Snowden*, Hot Books, 2016.
RAWLS J., *Théorie de la justice*, Seuil, 1987.
SCHNEIER B., *Secrets et mensonges : Sécurité numérique dans un monde en réseau*, Vuibert Informatique, 2017.
SCHWEITZER S., *Un chemin dissident : l'intérêt général ou l'invention d'un faux concept, in Les métamorphoses de l'intérêt général* (pp. 191-207), Presses Universitaires de l'ICES, 2013.

Encadré 1 - Lanceurs d'alertes : définition et exemple de Wikileaks

Le terme de lanceur d'alertes (de l'anglais "whistleblower", littéralement celui qui siffle le signal de détresse) est aujourd'hui bien connu, et son acception assez large puisqu'on qualifie de lanceur d'alertes toute personne qui révèle au public, directement ou indirectement, des informations censées rester secrètes et dont le lanceur d'alerte estime que le public devrait en avoir connaissance. Les organisations qui souhaitent conserver secrètes lesdites informations sont aussi bien privées (entreprises, ONG) que publiques (administrations, gouvernement national ou local, etc.). Dans cet encadré nous nous en tiendrons aux informations émanant des gouvernements et institutions publiques, puisque ce sont à la fois les affaires les plus médiatisées, et celles dont la nature même intéresse directement le public, qu'il le veuille ou non, tandis que les éventuels méfaits d'institutions privées ne concernent souvent qu'une petite fraction du public, qui de surcroît peut choisir de couper tout lien avec ces acteurs privés qui ne s'imposent pas légalement à lui.

Pour comprendre la suite de l'histoire, il faut rappeler l'événement tragiquement fondateur que fut le 11 septembre 2001 et ses quatre attentats suicides coordonnés sur le sol américain, dont le plus fameux reste le double crash de deux avions Boeing dans les tours jumelles du World Trade Center sur l'île de Manhattan, à New-York. C'était la première fois que les Etats-Unis d'Amérique étaient directement attaqués sur leur sol métropolitain, hors de tout contexte de guerre officielle (contrairement à l'attaque sur Pearl Harbor par une puissance, le Japon, que chacun savait hostile et prête à entrer en guerre avec l'Amérique). La conjonction de la surprise, du bilan effrayant de 2900 victimes - l'attentat terroriste le plus meurtrier de l'histoire humaine - et du choc des images diffusées en direct sur toute la planète a fait de cet évènement une borne historique : il y a eu un avant et un après 11 septembre. La réponse américaine fut proportionnelle au choc encaissé : un bouleversement législatif et deux guerres au Moyen-Orient qui auront duré près de dix ans. Dans un moment de grâce pour le gouvernement, les forces de police, l'armée et dans une certaine mesure les services de renseignement, l'opinion publique américaine a donné un quasi blanc-seing à ses dirigeants pour prendre toutes les mesures capables d'empêcher un nouveau 11 septembre. Et malgré des polémiques sur l'incapacité des services de renseignement à prédire la quadruple attaque, la réaction ne fut pas tant un rejet du renseignement qu'une demande pour plus de moyens à ces institutions.

L'organisation Wikileaks, fondée en 2006 par le hacker australien Julian Assange et l'allemand Daniel Domscheit-Berg, s'est en grande partie construite en réaction à cette importance accrue de l'appareil de surveillance et de répression du terrorisme suite aux attentats de 2001. Wikileaks s'est fixé pour objectif de permettre à tous les aspirants "lanceurs d'alertes" de transmettre des documents le plus souvent confidentiels tout en leur assurant l'anonymat sans lequel la peur du retour de flamme réduirait au silence la plupart des citoyens moyens. Partant du présupposé qu'on ne peut jamais faire une confiance totale et aveugle aux gouvernements pour ne pas abuser des pouvoirs étendus qui sont aujourd'hui les leurs, Assange et son organisation prétendent rétablir l'équilibre des pouvoirs en faveur du public. Le préfixe "wiki", généralement utilisé pour désigner les plateformes collaboratives et horizontales, vient de ce que Wikileaks fut dans un premier temps construit comme une plateforme collaborative, avant de se transformer assez rapidement en plateforme fermée et contrôlée par une poignée de responsables seuls habilités de décider quels documents pourraient être révélés. Cette évolution semble naturelle au vu des risques que présentait une architecture trop ouverte, que ce soit pour les lanceurs d'alertes ou pour l'équipe de Wikileaks.

Après avoir commencé à faire quelques vagues avec des scandales comme l'existence "d'escadrons de la mort" au Kenya, ou encore la connivence des responsables politiques en Islande après la banqueroute du système bancaire de leur pays (dans le sillage de la crise des subprimes en 2007-2008) c'est en 2010 que le monde entier découvre l'impact que peut avoir Wikileaks avec la publication de la vidéo "Collateral Murder" (meurtre collatéral). La vidéo, prise depuis un hélicoptère de combat américain à Bagdad, montre des soldats ouvrant le feu sur un groupe de civils parmi lesquels deux journalistes de l'agence de presse Reuters, alors que ces derniers sont clairement identifiés comme tels. Plus troublant, alors qu'un père de famille qui accompagnait ses enfants à l'école s'arrête pour porter secours aux blessés, les soldats tirent de nouveau sur le groupe (les enfants en réchapperont, mais pas leur père). Au-delà de l'acte, c'est le rire des soldats qui se félicitent de leurs tirs comme s'ils jouaient à un jeu vidéo ("et boum, en plein dans le pare-brise !") qui créent la polémique. Cette vidéo est suivie de près par la publication des carnets de bord de l'armée américaine en Irak. L'étude de ces "War Logs" révèle ou documente d'autres pratiques non-officielles telles que la torture dans les prisons américaines sur le sol irakien, ainsi qu'une tendance à systématiquement user du terme « insurgé » pour désigner toute personne ayant été abattue à raison ou à tort par des soldats américains, un procédé commode pour effacer tout risque d'accusation de bavure. Pour enfoncer le clou, Wikileaks publie également un manuel d'opérations qui révèle des pratiques de torture dans le camp d'internement administratif de Guantanamo, où depuis près de quinze ans des détenus sont emprisonnés pour une durée indéterminée, sans accusation ni procès, contre toutes les règles juridiques internationales. Enfin le scandale du "Cablegate" voit la publication de milliers de câbles diplomatiques entre le gouvernement américain et ses ambassades dans le monde entier, révélant les dessous peu reluisants de la diplomatie internationale avec son lot d'espionnage, de compromissions, et de petits arrangements. Ce dernier scandale a valu à Wikileaks des accusations de mise en danger des informateurs étrangers travaillant pour le compte des Etats-Unis, dont les noms n'ont pas été retirés des documents malgré les demandes de collaborateurs d'Assange qui se sont régulièrement heurtés au refus de ce dernier.

L'administration américaine a réagi en intentant des procédures judiciaires à l'encontre de Julian Assange et de sa principale source, le soldat Bradley Manning, qui a été confondu par les enquêteurs américains, jugé et condamné à 35 ans de réclusion dans un régime carcéral d'une extrême sévérité (Manning a tenté de se suicider en 2016, avant d'être libéré l'année suivante). Sous la pression du gouvernement, les opérateurs bancaires Visa, Mastercard et Paypal ont tous révoqué les comptes de l'organisation Wikileaks, participant à son asphyxie financière. Aujourd'hui Wikileaks passe par des organismes relais pour récolter les dons[52], et accepte la monnaie électronique Bitcoin qu'aucun gouvernement ne peut contrôler. Daniel Domscheit-Berg s'est éloigné de Wikileaks suite à des désaccords sur les méthodes de Julian Assange, et ce dernier a depuis été inquiété dans une affaire d'agression sexuelle en Suède. Craignant que la Suède ne l'extrade vers les Etats-Unis où il risque la peine de mort, Julian Assange a envoyé de nombreuses demandes d'asile qui ont été refusées par les pays alliés des Etats-Unis dont la France et le Royaume-Uni. C'est la République d'Equateur qui abrite aujourd'hui Assange dans son ambassade de Londres, où la police britannique monte la garde en permanence pour l'arrêter dès qu'il mettra un pied dehors, ce qui rend matériellement impossible une fuite vers l'Equateur ou tout autre pays qui accepterait de lui accorder le droit d'asile. L'ONU a officiellement dénoncé cette situation, sans résultat[53]. En 2018 la justice américaine divulgue par erreur un document mentionnant une procédure de poursuite judiciaire secrète contre Julian Assange[54], tandis que la justice britannique agit avec un

[52] En France l'organisme partenaire de Wikileaks est la FDN2 (Fonds de Défense de la Neutralité du Net) - http://www.fdn2.org

[53] Décision No. 54/2015 du Groupe de Travail des Nations Unies sur la Détention Arbitraire, en date du 5 février 2016.

[54] Le Monde/AFP/Reuters, 16 novembre 2018 https://www.lemonde.fr/pixels/article/2018/11/16/wikileaks-des-procureurs-revelent-par-erreur-l-inculpation-de-julian-assange-aux-etats-unis_5384250_4408996.html . Le document original est

zèle inhabituel[55] contre le fondateur de Wikileaks, confirmant ainsi les craintes de ce dernier d'être extradé aux Etats-Unis aussi

consultable à l'adresse suivante : https://pacer-documents.s3.amazonaws.com/179/399086/18919235200.pdf

[55] Le Monde, 5 février 2019. https://www.lemonde.fr/pixels/article/2019/02/05/depuis-2010-julian-assange-face-a-la-pression-plus-ou-moins-discrete-de-la-justice-britannique_5419597_4408996.html

Encadré 2 – L'affaire Edward Snowden

En 2013, à peine un an après la mise hors de la circulation de Julian Assange et alors que Wikileaks semble en perte en perte de vitesse, survient le second plus grand scandale lié aux lanceurs d'alertes avec les révélations d'Edward Snowden sur les méthodes de surveillance de masse utilisées par la NSA, l'agence de sécurité nationale américaine. Ingénieur en systèmes d'information, Snowden travaillait alors comme consultant sous-traitant pour la NSA. C'est alors qu'il réalise que la réalité de la surveillance des communications électroniques effectuée par l'agence américaine outrepasse de loin son mandat, ne fait l'objet d'aucun contrôle par les contre-pouvoirs politiques, et surtout inverse la logique du renseignement. Le programme PRISM en est un bon exemple, puisqu'il consiste à amasser de grandes quantités de données issues de communications électroniques à des fin d'exploitation présente ou future, mais sans besoin d'aucun soupçon d'activité illégale des personnes surveillées. Edward Snowden décide alors de révéler au public la nature et l'étendue de ces activités illégales, jugeant que le public doit savoir ce que font son gouvernement et ses agences en son nom. Selon lui on est en train de construire la plus grosse machine répressive de l'histoire, et celle-ci pourrait bien échapper à ses créateurs si les pouvoirs du renseignement continuent à s'accroître *de facto*. Il entreprend alors de copier illégalement des millions de documents informatiques, autant de preuves qu'il va transmettre en partie à des journalistes d'investigation tels que Glenn Greenwald de The Guardian, ou la réalisatrice française Laura Poitras, pour informer l'opinion américaine et internationale. Minutieusement orchestrées, « l'alerte est lancée » depuis une chambre d'hôtel à Hong-Kong. La machine diplomatique américaine ne tarde pas à réagir, et Snowden décide de demander l'asile politique à des nombreux pays, dont la France, qui comme beaucoup d'autres lui répond par la négative. Le lanceur d'alertes est en transit à l'aéroport de Moscou lorsque son passeport est révoqué, ce qui le place dans une situation administrative délicate avant que la Russie ne lui accorde l'asile politique.

Si des comparaisons ont souvent été faites entre Julian Assange et Edward Snowden, leur démarche et leurs objectifs semblent différer sensiblement. Si le premier est un partisan de la transparence totale, opposant assumé à tous les gouvernements, habitué aux actions illégales pour peu qu'il les juge légitime, Snowden est au contraire un produit du système, partisan de la légalité et de l'ordre gouvernemental tant que les règles sont respectées. Assange a créé la polémique jusque chez ses collaborateurs en refusant catégoriquement d'altérer des documents pour protéger certains informateurs de possibles représailles, tandis que Snowden a privilégié une sélection des documents en accord avec des journalistes et dans un souci de sécurité plutôt qu'une publication en masse et sans précautions. Assange est critiqué pour sa personnalité froide, autoritaire, tyrannique et egocentrique selon certains, alors que Snowden est un personnage discret, d'apparence modeste et nettement moins radical qu'Assange[56], ce qui ne le met pas moins en danger face à la justice américaine.

Barack Obama et Hillary Clinton ont vertement critiqué la démarche d'Edward Snowden, soulignant qu'il avait délibérément opté pour la voie de presse au lieu d'alerter sa hiérarchie, quitte à bénéficier de la législation américaine de protection des lanceurs d'alertes. Snowden assume ce choix et le justifie par le précédent inquiétant de Thomas Drake et John Crane. Ces deux personnages haut placés respectivement à la NSA et au Pentagone (Ministère de la Défense) ont chacun tenté d'emprunter les voies légales pour faire part de leur inquiétude sur la légalité, la faisabilité

[56] Cette opinion est notamment partagée par Laura Poitras, réalisatrice des documentaires Citizen Four et Risk, respectivement consacrés à Snowden et Assange. Elle se montre très critique face à Assange, tout en reconnaissant que son travail aura été bénéfique au total.

financière, les risques de dérive et d'inefficacité des actions de renseignement. Ils ont tous deux été brisés de manière tellement claire que Snowden a perdu d'avance tout espoir de réformer le système de l'intérieur, une approche qui aurait pourtant eu le double avantage de couper court à la polémique sur le bien-fondé du vol de documents classifiés tout en lui conservant une protection juridique, au moins théoriquement. Les chances d'obtenir le moindre changement notable lui ont paru tellement faibles qu'il a préféré rendre l'affaire publique en sachant par avance qu'il serait traqué sans relâche.

En février 2019, Edward Snowden est toujours réfugié en Russie, où il affirme mener une vie relativement normale bien que discrète. Son temps est largement consacré à la poursuite de son combat pour la protection de la vie privée, qu'il mène en tant que président de la Freedom of the Press Foundation. Profitant des possibilités offertes par Internet, il participe à distance à de nombreux événements et interviews depuis son lieu d'asile. Après l'affaire des Panama Papers début 2016, la France plaidé en faveur d'une protection renforcée des lanceurs d'alertes, sans pour autant ouvrir la porte à l'asile politique pour Edward Snowden. Ce dernier a alors souligné l'incohérence de la position du Président François Hollande[57].

Pierre Schweitzer
Maître de Conférences Associé
Aix-Marseille Univ
Laboratoire Interdisciplinaire de Droit des Médias et des Mutations Sociales – EA4328

[57] Le 5 avril 2016, sur Twitter, Edward Snowden réagit à un tweet de Cnews citant François Hollande (.@fhollande sur les #PanamaPapers > "Il faut protéger les lanceurs d'alerte, ils font un travail utile et prennent des risques") avec le commentaire suivant - en français dans le texte - : « Vraiment ? »