Numérique et raison d'État : doit-on tout savoir ?

par

Pierre SCHWEITZER

En même temps que les points de vue dominants sur le marché des idées, le paradigme technologique d'une époque définit également et directement la manière dont l'État assure sa domination sur la population qui se trouve sous son contrôle. Nous pourrions remonter jusqu'à l'invention de l'écriture, mais pour un exemple plus pertinent et plus proche il suffira d'évoquer l'invention de l'imprimerie au XV^{e} siècle et son influence sur la diffusion de la réforme protestante et de la pensée humaniste, qui constituèrent pour la monarchie d'alors – dont la légitimité était essentiellement très étroitement liée au catholicisme et dont l'autorité était fortement relayée par l'Eglise Catholique - une menace réelle de diminution de son emprise sur la société toute entière.

L'une des justifications de la délégation de pouvoir aux hommes et femmes de l'État tient au niveau d'éducation et d'information dont disposent ces derniers pour prendre des décisions éclairées s'appliquant à l'ensemble de leurs sujets ou concitoyens. Concrètement ce pouvoir est d'autant moins menacé que d'une part le niveau d'information de la population est maintenu au plus faible et/ou au contenu finement censuré, et que d'autre part les possibilités de coordination entre dissidents du régime sont limitées. Aux temps modernes l'évolution des technologies de communication et d'information a changé la donne, créant les conditions favorables pour des changements politiques majeurs tels que l'avènement de la République. Mais si les moyens de coordination entre dissidents se sont améliorés, les moyens de communication entre cellules du pouvoir de l'État réparties sur un territoire donné ont progressé dans les mêmes proportions, renforçant le pouvoir de surveillance et de répression pour contrecarrer les progrès de la dissidence. L'information circulant sur

papier, puis par ondes hertziennes n'est pas encore parfaitement fluide et demeure largement saisissable, et le pouvoir ne s'est jamais privé d'intercepter et faire interdire des écrits lorsque ces derniers ne lui convenaient pas, y compris dans des époques très récentes. Ainsi par exemple, même si finalement il y a renoncé, on sait que le président Valéry Giscard d'Estaing a projeté de capturer des sources pour interrompre le flux d'informations gênantes à son endroit à propos de l'affaire des diamants de Bokassa. Mais l'exemple récent le plus spectaculaire est la façon dont, au-delà même des cellules d'écoute élyséennes, le président François Mitterrand a réussi à interdire *de facto* l'impression et la diffusion du livre de Jean-Edern Hallier, livre dans lequel l'écrivain démontrait l'existence d'une fille cachée du président mais surtout son installation dans un palais de la République avec l'ensemble des dépenses nécessaires pour assurer la protection de l'enfant en question. La persécution systématique et violente de l'écrivain l'amena à des extrémités tragiques. Mais on sait qu'en la matière le sillon français est particulièrement fécond puisque Philippe Le Bel, Richelieu, Colbert, Fouché, Talleyrand et bien d'autres ne se sont jamais privés au nom de l'intérêt général de violer les droits les plus élémentaires. Les plus candides s'étaient imaginés que les institutions républicaines mettraient fin à ce genre de pratiques.

L'avènement des technologies numériques dans toutes les couches de la population a rendu l'information – au sens large, c'est à dire tout ce qui relève de l'esprit et peut être numérisé à l'aide de codage binaire[1] – intégralement fluide, et l'alliance avec Internet de toutes formes d'expression numérisable (texte, son, image, vidéo) en a fait une arme pratiquement insaisissable par les autorités. Nous sommes aujourd'hui dans la phase où les gouvernants cherchent des réponses adaptées à la révolution numérique et à la menace qu'elle représente pour leurs intérêts. A ce stade il est important de préciser que nous considérons les intérêts des gouvernants comme n'étant pas nécessairement identiques à ceux de leurs administrés. La « classe » politique est une somme d'individus qui ont chacun une éthique qui leur est propre, une vision différente de ce qu'est le bon

[1] Depuis les premiers temps de l'informatique on a fait usage du codage de l'information en base binaire. Il consiste à utiliser deux états (représentés par les chiffres 0 et 1) pour coder les informations et donner des instructions aux ordinateurs.

gouvernement, et surtout chacun est plus ou moins prêt à sacrifier un supposé intérêt général (ou du moins majoritaire) à son propre intérêt, y compris dans certains cas le plus bas intérêt pécuniaire. Certains préfèrent l'ordre à la liberté, d'autres sont beaucoup plus attachés aux droits fondamentaux des citoyens, y compris lorsque ces droits donnent à l'administré la possibilité de se défaire de l'emprise du gouvernement si ce dernier ne remplit plus la mission pour laquelle on l'a mandaté. Toute généralisation des intentions ou des pratiques serait exagérée, mais l'étude de plusieurs cas concrets nous permettra au moins de réfléchir sur les dérives de la surveillance de masse ou de l'extrême transparence.

L'opposition qui se manifeste parfois entre le respect du droit de certains citoyens et la poursuite de l'intérêt de certains autres peut amener l'État à ignorer sciemment le droit des premiers, et à s'autoriser une action contre eux. C'est ce qu'on appelle couramment la « raison d'État », soit le principe au nom duquel un État s'autorise à violer le droit en vertu d'un critère supérieur. A mesure que nous sommes passés de la monarchie à l'État de droit, le nombre de droits à respecter tant du côté des individus que du côté des hommes et femmes de l'État n'a fait qu'augmenter. Simultanément, la publicité donnée aux cas de violation de ces mêmes droits s'est appuyée de manière croissante sur les moyens de communication modernes. On notera avec intérêt que la dénonciation des manquements de l'État à ses propres règles est systématiquement soulignée, alors que les manquements des individus à leurs obligations le sont moins. L'explication est aisée : on attend des représentants de l'intérêt général l'exemplarité, aussi toute entorse est-elle dénoncée. Cette révolte devant la corruption du droit trouve évidemment son origine dans le fait suivant : c'est avec l'argent de l'impôt que les hommes et femmes de l'État pratiquent leurs interventions. Aujourd'hui nous sommes quasiment au paroxysme du conflit relatif au respect des droits dévolus aux uns et aux autres. Ainsi donc il nous faut, plus que jamais, nous reposer l'éternelle question des droits que nous sommes prêts à sacrifier au bon fonctionnement de l'État. Un État dont nous avons tendance à attendre toujours plus, particulièrement en matière de sécurité.

Pour aborder cette question nous adopterons une double grille de lecture : avant tout l'éthique, ou est-il juste de tolérer l'abandon de nos droits pour la raison d'État, et dans une moindre mesure l'utilité, ou est-il efficace de donner toujours plus de moyens de

surveillance à l'État pour mieux assurer notre sécurité ?

Pouvons-nous faire confiance à l'État pour utiliser sagement, et seulement en dernier recours, la violation du droit auquel il est soumis autant qu'il nous soumet, et ce au nom d'un critère supérieur ? Si nous partons du principe hypothétique qu'en règle générale le pouvoir de l'État est utilisé à bon escient, il paraît normal de se concentrer en priorité sur les cas où des abus de la raison d'État ont pu être mis au jour. Deux controverses concentrées sur la décennie en cours vont nous servir d'illustrations : l'affaire des « War Logs » révélée par Wikileaks, et l'alerte lancée par Edward Snowden sur la surveillance de masse par une agence de l'État américain.

En 2010 le monde entier apprend l'existence d'une plateforme Internet baptisée Wikileaks à l'occasion d'un scandale d'ampleur mondiale sur les dérives de l'armée américaine durant la seconde guerre d'Irak . Le nom même de Wikileaks donne le ton : il s'agit d'un site qui se voulait au départ collaboratif (d'où le terme de « wiki » qui fait référence au logiciel libre permettant de réaliser des sites d'information colloboratifs ou des encyclopédies collaboratives telles que Wikipédia), et centré sur les fuites d'information (d'où le terme « leaks », terme anglais pour désigner une fuite). Toutefois le site a rapidement perdu sa nature librement collaborative et s'est mué en un lieu où tout un chacun pouvait seulement proposer aux éditeurs, de manière anonyme, des documents considérés comme sensibles. L'équipe de Wikileaks étudiait ensuite lesdits documents pour publier ceux qu'elle considérait comme authentiques. Le journaliste australien Julian Assange a rapidement pris l'ascendant sur ses collaborateurs des débuts, notamment l'Allemand Daniel Domscheit-Berg[2]. De fait c'est Julian Assange qui incarne seul Wikileaks, bien que l'organisation compte des collaborateurs dont le nombre exact est inconnu et qui restent discrets par peur des représailles gouvernementales qui se sont abattues depuis 2010 dans

[2] Cette collaboration alternant entre admiration, méfiance et rivalité est bien restituée dans le film « Le Cinquième Pouvoir » (The Fifth Estate), sorti en 2013 et réalisé par Bill Condon, avec Benedict Cumberbatch dans le rôle d'Assange. Le vrai Julian Assange a toutefois exprimé son scepticisme quant à cette version des faits, et n'a pas souhaité apporter son concours à l'équipe du film. De fait, le film écorne le mythe en peignant le portrait d'un Assange aux tendances paranoïaques, mythomanes et mégalomanes.

plusieurs pays sur toutes les personnes se revendiquant ouvertement de Wikileaks.

C'est une forme de journalisme peu commune que pratique Wikileaks, puisque la publication des documents se fait systématiquement dans leur forme brute, sans aucun filtrage à partir du moment où le document est considéré comme fiable. C'est un principe auquel tient particulièrement Assange. C'est la raison pour laquelle des dizaines de grands médias internationaux ont apporté leur concours pour éplucher les documents bruts et en tirer une véritable information compréhensible par le grand public. C'est ainsi que des journaux comme Der Spiegel, The Guardian, The New-York Times ou encore Le Monde ont aidé Wikileaks pour faire connaître au public les fameux War Logs et ce qu'ils pouvaient contenir d'intéressant. Ce que les War Logs ont révélé de notable n'est rien de moins que l'existence de crimes de guerre commis par l'armée américaine sur le sol irakien. Parmi plusieurs exemples, le plus célèbre demeure cette vidéo qui montre des soldats américains tirer à vue sur un groupe de civils - dont deux journalistes de l'agence de presse Reuters - pourtant clairement identifiables comme tels. Après les premiers tirs on entend les soldats plaisanter entre eux et s'amuser à abattre les survivants au milieu des rires, alors que parmi ces survivants, dont certains rampaient pour leur vie contre le trottoir, figuraient des enfants. La vidéo est d'une violence difficilement supportable, et sa diffusion a naturellement fait l'effet d'une bombe dans un contexte où la propagande américaine peinait à justifier une guerre qui durait déjà depuis sept ans et dont les résultats tardaient à venir. L'étude des War Logs révèle ou confirme d'autres pratiques contestables 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 bienvenu pour effacer tout risque d'accusation de bavure.

Si l'affaire fut en soi intéressante, la réaction du gouvernement américain le fut peut-être plus encore. Au lieu d'admettre des erreurs et de promettre de changer son attitude sur les théâtres d'opérations, les plus hauts personnages de l'État, jusqu'au président Obama en personne, se déchainèrent littéralement contre Wikileaks et Julian Assange au prétexte que ces derniers auraient révélé des documents auxquels ils n'auraient jamais dû avoir accès. Wikileaks se

vit accusé d'avoir délibérément affaibli le prestige et la position de l'armée américaine en Irak en la livrant au feu des critiques du monde entier. C'était annihiler ainsi les efforts colossaux précedemment entrepris par les États-Unis pour faire accepter cette guerre à l'opinion au travers d'une présentation d'un manichéisme grossier dont les géopoliticiens et véritables spécialistes de la guerre savent bien qu'il est inopérant pour décrire fidèlement la réalité irakienne. Depuis 2010 Julian Assange vit sous la menace de poursuites pénales graves aux États-Unis, une situation peu enviable et nettement compliquée par sa mise en accusation en Suède pour agression sexuelle sur deux femmes. Assange nie la réalité de ces allégations et ne se prive pas pour accuser ses détracteurs d'avoir manipulé les accusatrices qui, de fait, ont tardé à se manifester et ont attendu la grande affaire des War Logs pour se décider. L'accord d'extradition existant entre la Suède et les États-Unis fait craindre à Assange de se retrouver devant une justice américaine dont il espère peu d'indépendance tant le gouvernement a voulu le présenter comme un criminel, allié objectif des terroristes et des ennemis de l'Amérique, et a réussi à faire adhérer une partie de l'opinion publique à cette vision. C'est pourquoi en 2012, alors qu'il vivait en résidence surveillée au Royaume-Uni et ayant appris sa probable arrestation pour l'extrader vers la Suède, Julian Assange a demandé l'asile politique à des pays du monde entier (la France a refusé) et a finalement décidé d'accepter l'hospitalité et la protection diplomatique de l'ambassade de la République d'Equateur à Londres. Cela fait donc près de quatre années que le fondateur de Wikileaks vit reclus dans une ambassade qui n'est rien de plus qu'un appartement, et n'a pas pu faire un seul pas dehors sachant que la police britannique monte la garde jour et nuit et s'apprête à lui passer les menottes dès la porte franchie. Le gouvernement américain a donc choisi de s'acharner sur le messager – ce qui peut certes se comprendre de son point de vue – mais n'a pas semblé aussi choqué par le message, nous conduisant donc à penser que parfois l'État a ses raisons que l'éthique ignore, et consacre plus d'énergie à se protéger contre tout procès en violation de droits qu'à faire en sorte que ces violations elles-mêmes se limitent aux cas extrêmes qui engagent la survie de l'État et de la nation.

Notre second exemple est celui du lanceur d'alerte Edward Snowden et de ses révélations fracassantes sur les pratiques de violation de la vie privée de millions de personnes par les services de

renseignement américains. Le parallèle avec l'exemple de Wikileaks est saisissant. Nous sommes à l'été 2013, dans un contexte plus que jamais marqué par le terrorisme mondial et les fléaux modernes que sont Al-Qaida et ses branches locales plus ou moins autonomes comme AQMI en Afrique du Nord. C'est alors que des journaux américains sont contactés par un jeune ingénieur informaticien d'une trentaine d'années, ancien agent de la National Security Agency (agence gouvernementale américaine chargée de la sécurité intérieure). Edward Snowden a des révélations à faire sur des pratiques illégales de surveillance par collecte massive de données privées à des fins de renseignement et de fichage. Ses allégations sont appuyées de très nombreux documents empruntés à l'agence au temps où il y travaillait, mais divulgués de manière naturellement illégale. Un procédé jugé incontournable par Snowden pour faire savoir au monde des violations légales autrement plus graves. On y apprend que la NSA, au lieu de pratiquer du renseignement ciblé avec des données obtenues légalement, a souvent opté pour un ramassage « au chalut » de millions de données prises sans autorisation légale, conservées et exploitées tout aussi illégalement. Profitant de la psychose sécuritaire qui a suivi le 11 septembre 2001, les agents de l'État se sont sentis pousser des ailes et ont profité de la confiance et du manque de vigilance des contre-pouvoirs institutionnels, ce qui a eu pour effet de mettre excessivement en confiance la NSA pour exercer son mandat hors des limites fixées par les représentants de la nation. Comble de cynisme, la NSA n'a pas hésité à mettre sur écoute téléphonique des personnalités étrangères établies sur le sol étranger, parmi lesquelles des dirigeants politiques européens de premier plan. Le gouvernement américain fût doublement embarrassé par la facilité avec laquelle des documents de l'agence chargée de la sécurité intérieure avaient pu être dérobés et rendus publics, mais aussi par les pratiques décrites dans lesdits documents. Toutefois, c'est une fois de plus sur le messager (que ses partisans qualifient de « lanceur d'alerte ») que l'État a concentré ses efforts de répression, jugeant peut-être que remettre en cause et discréditer une agence de l'État était un crime plus grand que celui consistant pour l'agence à désobéir à sa propre autorité de tutelle et surveiller des millions d'honnêtes citoyens dans le cadre du programme PRISM. Certains éditorialistes et parlementaires conservateurs allèrent jusqu'à demander au gouvernement d'envoyer un drone de combat pour assassiner Edward Snowden sans autre forme de procès, comme les États-Unis

ont l'habitude de procéder avec les terroristes notoires. Côté démocrate la position était moins violente mais similaire sur le fond : l'ancien ingénieur de la NSA n'était qu'un vulgaire traître à la nation, et sûrement pas un lanceur d'alerte. Dans sa fuite pour échapper à un procès à l'issue potentiellement très sévère pour lui, Snowden demandera l'asile à de nombreux pays dont la France, qui le lui refusera, comme pour Julian Assange[3]. Finalement c'est la Russie de Vladimir Poutine qui se paiera le luxe d'adopter une position de protectrice des lanceurs d'alerte menacés par une grande démocratie occidentale pour avoir révélé des pratiques contraires à ses propres lois. Aujourd'hui Edward Snowden est devenu une icône pour tous les défenseurs des citoyens contre les abus du pouvoir de l'État, il intervient régulièrement à distance – grâce aux technologies numériques sur lesquelles les gouvernements ont peu de prise - dans des congrès prestigieux et manque rarement de commenter les dérives de la surveillance policière dans un contexte de lutte effrénée contre le terrorisme. Comme on l'a constaté, l'Amérique a plus été choquée par la méthode de révélation des abus de la NSA que par la nature et l'étendue de ces abus commis systématiquement depuis de nombreuses années. Certains ont relevé l'ironie d'une situation où un prix Nobel de la Paix (le président Obama) a déployé tout l'appareil d'État pour traquer et tenter de capturer un autre candidat à ce même Nobel, bien que ne l'ayant pas obtenu.

Tenant donc pour vrai qu'il arrive à l'État de dépasser gravement le mandat qui lui est donné en matière de surveillance des communications électroniques, sur quels arguments éthiques s'appuie-t-il pour en faire accepter le principe ?

Il ne serait pas intellectuellement honnête de se limiter à l'État

[3] En avril 2016, à l'occasion du vaste scandale des Panama Papers, la question de la protection des lanceurs d'alertes est revenue au premier plan. Le Président Hollande a souligné l'importance des lanceurs d'alerte et la nécessité de les protéger. Snowden, toujours réfugié en Russie, s'est alors amusé de cette déclaration d'intentions visiblement non suivie d'effets pour ce qui le concerne, en twittant « Vraiment ? » en français dans le texte. Il est vrai que le scandale des Panama Papers pourrait rapporter gros à l'administration fiscale tandis que le pot-aux-roses révélé par Snowden trois ans auparavant mettait en cause des acteurs publics et non privés. Faut-il y voir une explication des positions apparemment inconsistantes du gouvernement français ?

lorsqu'on parle de surveillance des communications électroniques et de collecte de données. De fait les entreprises privées du secteur numérique sont passées maîtresses dans l'art de collecter des données sur tous leurs utilisateurs afin d'établir des profils de consommateurs. Prenons Google, la plus grosse capitalisation boursière au monde au moment où nous écrivons[4], et dont les services sur le web et les plateformes mobiles sont très majoritairement gratuits. Il est évident qu'il existe une contrepartie à cette gratuité, qui consiste à stocker et analyser toutes les recherches, la navigation, et les échanges électroniques de ses utilisateurs afin de cibler le plus précisément possible les publicités auxquelles ils sont soumis. C'est seulement au prix de cette étroite surveillance que Google est capable de monnayer ses espaces publicitaires au travers d'un business model et d'une tarification particulière qui ont fait de la firme de Moutain View la première entreprise du monde et le symbole de la nouvelle économie. Les hommes et femmes de l'État sont régulièrement montés au créneau pour dénoncer les pratiques de Google, dénonçant bien souvent un modèle supposé sournois et dans lequel le consommateur serait prisonnier sans le savoir, obligé de céder ses données personnelles souvent sans le savoir en échange de services présentés comme gratuits mais qui cacheraient mal le fait que c'est l'utilisateur qui serait en réalité le produit. Cependant s'il est incontestable que Google et les entreprises de son secteur (le réseau social Facebook repose par exemple sur un modèle très similaire, « données personnelles contre nombreux services ») disposent de très nombreuses données sur leurs utilisateurs, rendant la notion d'anonymat totalement obsolète, il existe des différences de taille avec les pratiques de l'État. D'abord en termes d'acceptation préalable : d'un côté l'utilisateur demande l'accès à des services pour lesquels il est tenu de signer préalablement des conditions générales d'utilisation, certes longues et rébarbatives, qui détaillent quelles données pourront être collectées et dans quel but. L'acceptation est individuelle et éclairée, au contraire de la surveillance effectuée par

[4] Pour une meilleure compréhension par le lecteur nous parlons de Google, toutefois Google n'est qu'une entreprise appartenant au groupe Alphabet, créé en 2015 pour englober les différentes entreprises qui dépendaient autrefois de Google. C'est donc Alphabet qui en 2015 est devenue la plus grosse capitalisation boursière au monde, détrônant son concurrent Apple.

l'État et qui n'est acceptée que de manière majoritaire, indirecte et non éclairée. Un citoyen qui n'a pas voté pour le gouvernement en place peut néanmoins se voir imposer une surveillance légalisée par ce gouvernement et dont il ne connaît ni l'étendue exacte ni la profondeur, et il n'obtient aucun service comparable à Google en échange, si ce n'est la promesse très incertaine d'une meilleure sécurité. Deuxièmement il est possible pour l'utilisateur qui souhaite renoncer aux services de Google ou Facebook de supprimer définitivement son compte ainsi que l'ensemble des données stockées par le prestataire de services. Il faut toutefois faire crédit au législateur d'avoir su faire pression sur les géants du net pour obtenir cette possibilité qui n'allait pas de soi pour Google et comparses. Dans le cas de l'État il est naturellement impensable de changer de prestataire de sécurité intérieure, ni même de renoncer à la protection de l'État dans ce domaine. Nous sommes « prisonniers » des services de notre État, quel que soit notre degré de satisfaction quant à l'accomplissement de ses missions. Il est tout aussi impensable d'exiger que les agences de l'État se séparent de toutes les données dont elles disposent nous concernant. En résumé il est clair que dans un cas le consommateur est libre face à une entreprise avec laquelle il peut ou non contracter, tandis que dans l'autre cas il est prisonnier d'un État dont il ne peut sortir que s'il accepte de s'exiler et si un pays étranger veut bien lui accorder la citoyenneté. La différence est majeure et rend d'avance extrêmement peu pertinente toute comparaison entre les deux systèmes de collecte de données. Ajoutons enfin que l'État regrette moins la collecte de données par Google que l'impossibilité de profiter de ces données pour lui-même. Les connaisseurs du secteur numérique et de ses grandes entreprises s'accordent largement pour reconnaître que les gouvernements – en dictature comme en démocratie – exercent des pressions de plus en plus fortes pour accéder à l'ensemble des données dont disposent les entreprises telles que Google, Facebook, ou encore Apple. Certaines de ces dernières ont d'ailleurs publiquement reconnu que de telles demandes ont été formulées par la NSA ou le FBI, pour ne citer que les agences les plus connues.

Un autre argument du domaine de l'éthique est récurrent dans le débat sur la surveillance des citoyens. On pourrait le résumer ainsi : « si vous n'avez rien à cacher, alors vous n'avez rien à craindre ». Cet argument pourrait éventuellement tenir s'il était admis que l'État n'outrepasse jamais le mandat pour lequel il met en

place un système de surveillance, or les précédents exemples, tous deux récents, nous prouvent exactement le contraire. L'histoire plus ancienne est là pour nous rappeler que tous les régimes de terreur politique, de la Révolution Française au bolchévisme en passant par le Régime de Vichy, ont exploité des événements qui pouvaient effectivement justifier une étroite surveillance et des pouvoirs de police étendus, mais que progressivement la police est devenue politique et que des innocents ont payé de leur vie l'acceptation d'un système de surveillance qui se voulait initialement, du moins officiellement, bienveillant et proportionné. A l'époque des terribles lois du 22 Prairial An II, privant de procès tous les « ennemis de la liberté » et réduisant le pouvoir judiciaire à une chambre d'enregistrement des condamnations à mort décidées par l'éxécutif, Robespierre pouvait bien tenter de rassurer les conventionnels avec sa célèbre formule « en cet instant, seuls les coupables tremblent », il était pourtant évident que les morts de la guillotine n'étaient pas tous « coupables »[5], même en se fondant sur les critères du Comité de Salut Public. Plus généralement la surveillance de masse est dangereuse car même instaurée par un gouvernement démocratique et respectueux de l'État de Droit, elle constitue une arme redoutable pour tout futur gouvernement moins regardant sur ce même État de Droit.

Un dernier argument éthique mérite ici d'être rappelé : il n'existe pas de réelle liberté d'agir sans un droit d'agir à l'abri du regard d'autrui. Nous n'entrerons pas ici dans les considérations sociologiques détaillées qui démontrent l'existence d'une influence des personnes de notre entourage sur nos actions privées au travers de leur jugement moral. S'il est vrai que l'évolution de l'organisation sociale vers plus de respect de l'individu et de sa liberté de mener la vie qu'il entend en privé (sexualité, habitudes considérées parfois comme des vices ou des déviances, croyances religieuses, préférences politiques, etc.) a favorisé une certaine émancipation de l'individu par rapport à la communauté et à l'ordre moral que celle-ci entend parfois imposer à tous ses membres, notre époque ne nous a pas mis à l'abri de toute forme de jugement social. On le voit avec la persistance des agressions antisémites, homophobes, islamophobes, etc. Ceci posé, on peut raisonnablement considérer que la

[5] Bien que l'on prête au bourreau Charles-Henri Sanson la formule selon laquelle tous les condamnés, après avoir fait le test sur la guillotine, s'étaient avérés littéralement « coupables ».

connaissance par l'autorité publique des habitudes de navigation d'un citoyen sur le web a une influence sur la liberté d'action de ce dernier. Il est donc à craindre que même lorsque la surveillance étatique est mise en place pour des motifs sécuritaires, les individus s'autocensurent par peur de l'utilisation future qui pourrait être faite de leur vie privée, ce qui est intolérable en démocratie. La surveillance de masse, même exercée par la plus raisonnable et la plus légitime des autorités démocratiques, n'est jamais sans conséquence sur la liberté des citoyens qui craignent pour leur liberté présente et future. Un dernier exemple, heureusement non encore réalisé, vient appuyer notre propos. Au cours de sa campagne pour l'investiture du Parti Républicain à l'élection présidentielle de novembre 2016, l'homme d'affaires Donald Trump a proposé une mesure de fichage administratif des citoyens américains de confession musulmane. Une campagne politique, on le sait, est le lieu de toutes les provocations et de toutes les outrances pour attirer l'attention et les suffrages, mais un tel degré dans l'outrance – dans un contexte de démocratie et d'égalité des citoyens devant le droit – ne laisse pas de nous interroger. Comment ne pas craindre l'utilisation future qui pourrait être faite d'une telle liste, si la démocratie américaine venait à vaciller un jour ? Comment croire que les citoyens américains de confession musulmane peuvent encore tenir des propos totalement libres dans leurs communications électroniques, sachant que la NSA y a un accès extensif et communiquera naturellement ces données à son gouvernement de tutelle si ce dernier venait à concrétiser son projet de fichage administratif sur une base religieuse ?

Toujours en s'en tenant à l'éthique et à ce que nous savons de l'histoire, on peut justement considérer que la surveillance que les citoyens exercent sur leur État est plus cruciale que l'inverse. De fait, lorsqu'un citoyen contrevient à la loi il commet un délit privé qui n'engage que lui-même ainsi que les personnes éventuellement lésées par son délit. Tandis qu'un représentant de l'État ou de ses agences vit de l'argent des autres, de tous les autres. Un quelconque délit, fût-il comparable à celui commis par un citoyen dépourvu de mandat ou de fonction publiques, est toujours plus condamnable du point de vue de la morale car il est commis par celui-là même qui prétendait surveiller ses administrés et leur imposer le respect de la loi. Un triste exemple nous a été fourni par l'ancien ministre du Budget du gouvernement de Jean-Marc Ayrault, Monsieur Jérôme

Cahuzac, qui au titre de son ministère était en charge de la lutte contre l'évasion fiscale mais s'est avéré être lui-même un fraudeur au fisc de longue date et pour des montants élevés, ce qui ne l'a pas gêné au moment d'accepter sa fonction de ministre.

Pour clore cette approche éthique il convient d'aborder le cas particulier de la diplomatie dans les relations internationales. D'un point de vue purement théorique et moral, on peine à voir de quel droit les citoyens qui ont donné mandat à un gouvernement pour gérer leur pays seraient privés d'un simple droit de regard sur l'action diplomatique de leurs représentants. Les décisions d'un État engagent l'ensemble de ses ressortissants, on comprendrait donc que ces derniers puissent accéder s'ils le souhaitent à l'ensemble des informations dont dispose la représentation diplomatique afin que le citoyen puisse juger en connaissance de cause. Cependant si la transparence diplomatique peut être considérée comme éthiquement souhaitable, sa concrétisation pose des problèmes insolubles du point de vue pratique. Que cela nous satisfasse ou non moralement, il est indéniable que le secret est la condition indispensable de la réussite de toute négociation d'importance, or qu'est-ce que la diplomatie sinon une permanente négociation dont dépend le sort des nations et de leurs habitants ? S'il est vrai que les scandales d'État ne manquent pas de ternir ponctuellement le prestige des diplomates, quiconque prétend abolir le secret des négociations au nom de la dénonciation de telles anomalies doit accepter l'idée que toute la diplomatie d'état à état doit disparaître au profit d'un autre système. Wikileaks n'a pas manqué de s'attaquer au domaine diplomatique, suivant son principe directeur selon lequel toute information doit être révélée au public. C'est l'affaire du Cablegate, la révélation par l'organisation de Julian Assange de 250.000 câbles diplomatiques en 2010, suivant de quelques mois l'affaire des War Logs.

Dans l'essentiel de ce travail nous avons adopté la grille de lecture de l'éthique, qui nous a amené à conclure qu'en dehors de cas très particuliers il n'est pas légitime pour un état de généraliser la surveillance des citoyens et de l'instaurer de manière préventive. Le contradicteur aura vite fait d'objecter que l'efficacité de la surveillance généralisée peut à elle seule justifier un tel système pour qui place l'utilité au-dessus de la morale. La seconde grille de lecture de notre sujet, en forme de conclusion, consistera donc à se demander quelle est l'adéquation entre la fin et les moyens mis en

place lorsque nous parlons de surveillance des comportements et des communications numériques. Force est de constater, à y regarder de près, que la surveillance des communications électroniques, même généralisée et forte de moyens financiers conséquents, est un outil assez faible pour contrer les attentats terroristes.

Rappelons premièrement que le terroriste, par définition, n'a pas le comportement de l'internaute moyen. Sachant qu'il est hors-la-loi, il va user de tous les moyens existants pour compliquer la tâche des agences de sécurité : anonymisation de son ordinateur, cryptage complexe de ses courriers électroniques, brouillage de sa navigation à l'aide de logiciels comme Tor. Autant d'artifices qui sont loin d'être le monopole des experts en informatique : tout un chacun, sous réserve d'y consacrer quelques heures de son temps, peut apprendre à se cacher sur Internet. Le terroriste, plus que tout autre, a fortement intérêt à se faire expert en dissimulation électronique. Cela ne lui coûte guère beaucoup d'argent, tout juste un investissement en temps.

Supposons toutefois que les autorités parviennent à détecter les individus dont le profil pourrait les faire soupçonner d'intentions terroristes, parviendront-elles à pousser plus loin leurs investigations jusqu'à arrêter les véritables terroristes ? Pour bien le comprendre nous prendrons un exemple chiffré. Supposez que sur une population de 37 millions d'individus, on estime que 3.000 sont des terroristes potentiels (0,008 %), une estimation qui semble raisonnable d'après ce que les experts veulent bien communiquer. Un système de détection fiable à 99 % (ce qui serait miraculeux et n'existe pas à ce jour), signifie qu'il va identifier 2 970 de ces terroristes et en laisser filer 30 mais cela signifie aussi qu'il va accuser à tort 369.970 innocents. Pour éliminer ces faux positifs qui représentent tout de même plus de 99% des alertes du système, il va falloir diligenter pas moins de 372.940 enquêtes approfondies[6]. Ainsi, au bénéfice de la détection des vrais terroristes, la logique oblige à retrancher le coût des centaines de milliers d'enquêtes approfondies, ainsi que le coût humain de ces vies partiellement brisées par des

[6] L'exemple chiffré est emprunté à Guillaume Nicoulaud qui l'a développé dans un article du journal en ligne Contrepoints. http://www.contrepoints.org/2015/04/12/204178-loi-sur-le-renseignement-le-mythe-de-la-surveillance-de-masse

accusations gravement infâmantes, qui peuvent faire perdre à un honnête citoyen son travail, ses amis, son honneur, son argent. Quoiqu'il en soit aucun pays, même dans le riche Occident, n'a aujourd'hui les moyens financiers de diligenter plusieurs centaines de milliers d'enquêtes approfondies quand on sait ce qu'une seule enquête exige en termes de moyens humains et financiers. A cela il faut ajouter la considération suivante : une poignée de terroristes qui passerait entre les mailles du filet suffirait toujours à faire planer la menace d'un nouvel attentat. Or le coût du terrorisme pour la société ne se limite pas au nombre de vies perdues ou aux dégâts matériels, il réside en grande partie dans le climat de peur que fait régner la simple possibilité d'un nouvel attentat. Et même avec des moyens financiers colossaux que nous n'avons pas, et des systèmes de détection extrêmement fiables qui n'existent pas à ce jour, on peut hélas considérer qu'au vu des nombreuses manières dont un attentat peut être commis et de la relative simplicité avec laquelle on peut assassiner des cibles parfaitement aléatoires (la quasi absence de sélection des cibles est une réalité du terrorisme en 2016), les terroristes les plus déterminés parviendront toujours à leur fin ultime en dépit des efforts de l'anti-terrorisme : inspirer la terreur à toute une population.

D'un point de vue pratique la surveillance généralisée pose un autre problème fortement pénalisant : la création de failles de sécurité sur lesquelles la criminalité peut prospérer plus facilement que jamais. Les entreprises de nouvelles technologies informatiques conçoivent des systèmes d'exploitation pour téléphones portables et ordinateurs de telle manière que les pirates de toute sorte ne puissent pas librement s'y introduire. Cela n'empêche pas les failles de sécurité, mais ces dernières sont évidemment involontaires et sont rapidement corrigées par les constructeurs. Les autorités de surveillance demandent quant à elles la création systèmatique de « backdoors », soit des portes dérobées qui permettent au détenteur d'une clé virtuelle d'entrer librement dans l'ordinateur ou le téléphone d'une personne donnée. Si l'avantage pour les autorités est évident lorsqu'il s'agit de fouiller un appareil saisi lors d'une perquisition ou après un attentat, l'inconvénient pour l'ensemble des utilisateurs de tels systèmes est la création d'une faille de sécurité majeure et délibérée. Les professionnels de la sécurité informatique savent que les pirates sont généralement en avance sur les autorités et il est presque inévitable que les clés d'accès aux portes dérobées des systèmes informatiques ne restent pas éternellement à l'abri

entre les mains de ces autorités. Et si des pirates s'emparent de telles clés d'accès à des millions de téléphones et ordinateurs – nous suivons ici la logique des autorités qui demandent une généralisation des portes dérobées à tous les appareils mis en vente sur le marché – il ne faut pas douter des conséquences désastreuses que cela pourrait avoir en termes de vol de données sensibles, chantage aux photos personnelles, usurpation d'identité, etc. Comme souvent c'est bien l'honnête citoyen qui risque d'être victime de telles dérives involontaires, puisque le moindre terroriste rigoureux aura pris soin d'installer un système d'exploitation modifié et hors d'atteinte des autorités.

Les précédents développements nous amènent à une conclusion très nette en défaveur de la surveillance des citoyens par leurs gouvernants. Il ne s'agit pas de nier l'utilité de l'activité de renseignement telle qu'elle a historiquement existé, c'est-à-dire le suivi d'individus ciblés sur des critères objectifs et dans les limites prévues par la loi, le tout sous contrôle vigilant d'un contre-pouvoir. Mais la méthode consistant à s'octroyer le droit de surveiller toutes les activités de communication électronique de tous les citoyens apparaît fortement contestable d'un point de vue éthique, tant pour le principe que pour les risques de dérive autoritaire voire totalitaire qu'elle porte en germe. Il apparaît tout aussi difficile de défendre la surveillance de masse à l'aune du critère de son efficacité, étant donné qu'aucun état pratiquant la surveillance de masse en réponse à de précédents attentats terroristes n'est parvenu à faire cesser durablement ces attentats. Pire, l'instauration d'une surveillance de masse met automatiquement les citoyens en danger puisque leurs données électroniques – c'est-à-dire une partie substantielle de leur vie – est exposée aux risques de récupération par des pirates ou encore aux risques d'utilisation abusive par les autorités présentes ou futures.

Pourquoi dans ces conditions la collecte massive de données parvient-elle encore à séduire de très nombreux gouvernants ainsi qu'une partie de l'opinion publique ? On peut penser que du point de vue des entrepreneurs politiques le coût des attentats terroristes sur leur crédibilité et leur popularité est tellement élevé qu'il vaut mieux adopter une solution d'apparence radicale en faisant mine de croire à son efficacité plutôt que d'avouer l'impuissance relative des hommes et femmes de l'État sur le problème du terrorisme. Le bénéfice d'adopter une loi d'apparence efficace contre le terrorisme est

concentré sur le personnel politique, tandis que les coûts d'un tel dispositif sont répartis sur tout le reste de la population mais ne sont aucunement supportés par les décisionnaires, créant une incitation évidente pour cette minorité gouvernante à choisir une solution dont les coûts risquent pourtant fortement d'excéder les bénéfices pour la majorité.

Les autres solutions, comme celles consistant à armer la population pour permettre une défense individuelle en cas d'attaque terroriste, seraient catastrophique pour les gouvernants puisqu'elles rééquilibreraient le pouvoir réel en faveur des gouvernés et au détriment des gouvernants. Or nous savons grâce à James Buchanan et Gordon Tullock que le propre de l'homme de pouvoir est de vouloir continuellement étendre son pouvoir, peu importe le bénéfice pour la majorité de la population. Ceci explique peut-être pourquoi les solutions qui valorisent le rôle de l'État seront toujours mises en avant au détriment des solutions où le citoyen prime.