Note :

Julien Assange et Edward Snowden n’ont rien en commun au niveau politique et au niveau de la personnalité. Ils s’étaient brouillés définitivement dès les premiers échanges écrits qu’ils avaient pu avoir.

● Julien Assange est un ancien jeune hacker Australien (1987) puis a fait des études et travaux d’informatique. Il était éditeur de WikiLeak co-créé en 2007 à partir de Suède, un outil qui se veut défendre le « droit de savoir », car sans informations les citoyen-ne-s ne peuvent pas juger. Wikileaks a travaillé avec *The Guardian*, *The New York Times*, *Der Spiegel*, *Le Monde ou El País*, le *Times*, *Médiapart*... ce qui a donné un énorme bonus à leur image (*Exclusif*!) d’une presse indépendante d’investigation. Depuis que Wikileaks a publié la collection de documents militaires classifiés des États-Unis sur la guerre en Afghanistan et les registres de la guerre en Irak en 2010 ce qui a déclenché les foudres du pentagone, l’"indépendance" des mêmes médias a disparue. WikiLeaks ne hacke pas. Les documents publiés lui ont toujours été fournis (pour l’armée américaine par la soldate Chelsea Manning). Julien Assange (qui n’a jamais été accusé de viol contrairement à ce qui est laissé croire) est en cours de destruction physique et psychologique en plein cœur de Londres sans préoccupation aucune de protestations de l’ONU et autres.

● Edward Snowden est un ancien « geek » américain de la côte Est. Il aime son pays les USA (ses deux parents travaillaient dans la surveillance étatique, et il s’était engagé dans l’armée à 20 ans suite à l’attentat du World Trade Center en 2001) et veut que son pays, et notamment ses services d’État, respecte sa constitution. Il s’explique dans *Permanent Record* dont ci-dessous des extraits. Il est obligé de vivre à Moscou parce que le gouvernement de son pays veut le flanquer en prison pour des décennies. Il est actuellement président du conseil d’administration de the *Freedom of the Press Foundation*, FPF.

Ces deux militants au caractère trempé ont ceci de commun, en dehors de leur passion des ordinateurs depuis un très jeune âge, qu’ils étaient conscients qu’ils s’attaquaient à très gros et prenaient un très gros risque. Chacun pour ce qui lui tient à cœur espérait et espère, que grâce à des éléments cachés d’importance qu’il a voulu et réussi avec grande difficulté à mettre au jour, faire bouger les choses.

Extraits du livre :

Edward Snowden, 2019

Permanent Record

Metropolitan book, New York

(autorisé aux USA mais l'État saisit tous les revenus du livre sur l'argument que les contrats d'emplois de E. Snowden n'autorisaient pas les publications sans autorisation...)

livre traduit en français, aux Ed. Le Seuil, sept. 2019, 382p., sous le titre différent de :

Mémoires vives

(NSA : National Security Agency)

p. 11.
« *Dans un tunnel creusé sous un champs d'ananas et qui abritait, à l'époque de Pearl Harbor, une usine où l'on construisait des avions, j'étais installé devant un terminal qui me donnait un accès quasi illimité aux communications de n'importe qui ayant composé un numéro de téléphone ou pianoté sur un ordinateur. Parmi eux il y avait les 320 millions d'Américains, mes compatriotes, qui étaient quotidiennement épiés, en violation flagrante non seulement des principes de la Constitution américaine mais aussi des valeurs fondamentales de toute société libre.* »

p. 13.
« *Les entreprises se son aperçues que ceux qui se connectaient cherchaient moins à dépenser de l'argent qu'à s'exprimer, et que ces connexions humaines rendus possibles par Internet pouvaient être monétisées. Si ce qui intéressait la plupart des gens était de raconter (et de lire) par ce biais à leur proches, à leurs amis ou à des étrangers ce qu'ils faisaient, les entreprises n'avaient plus qu'à trouver le moyen de se glisser dans leur conversations et en tirer profit.*
C'est ce qui a signé le début du capitalisme de surveillance et la fin de l'Internet tel que je l'avais connu. Le Web créatif s'est effondré et une multitude de sites magnifiques, singuliers et pas toujours facile à gérer ont fermé. Leur maintenance était laborieuse alors les gens les ont remplacés par une page Facebook ou un compte Gmail, plus commodes. Tout se passait comme s'ils en étaient propriétaires alors que ce n'était pas le cas. »

p. 129.
« *Entre autres documents que j'ai remis aux journalistes figurait le « budget noir » de 2013. Il s'agissait d'un budget secret dont 68 % du montant, soit 52,6 milliards de dollars, était affecté aux services de renseignement et notamment au règlement des salaires versés à ses 107 035 employés qui, pour 20 % d'entre eux (21 400 personnes), étaient des contractuels engagés à plein plein temps. Et encore ce chiffre ne prend pas en compte les dizaines de milliers de personnes supplémentaires employées par des sociétés privées ayant signé des contrats de sous-traitance portant sur des taches ou des projets bien précis. Ces contractuels ne sont jamais comptabilisés par l'État, pas même dans le « budget noir », car ça reviendrait à reconnaître de manière très claire une réalité gênante : au États-Unis, le travail de renseignement incombe aussi fréquemment à des employés du privé qu'à des fonctionnaires.* »
p. 135. « *Si j'étais officiellement employé par COMSO, je n'ai jamais travaillé dans ses locaux ni dans ceux de BAE Systems, et peu de contractuels y ont un jour mis les pieds. J'ai uniquement travaillé au quartier général de la CIA.* »

p. 173.
« *Ce nouveau monde du « renseignement numérique » ou des « opérations basées sur les réseaux informatiques » permettait de ne plus avoir besoin de se rendre sur les lieux, ce qui réduisait d'autant les risques encourus par les individus concernés et définissait un nouvel équilibre entre HUMINT et SIGINT. Un agent pouvait désormais se contenter d'envoyer un message ciblé, par exemple un e-mail, dont les pièces jointes et les liens déclenchaient un programme malveillant grâce auquel la CIA pouvait surveiller l'individu ciblé mais également son réseau entier.* »

p. 183.
« *Internet est fondamentalement américain mais il m'a fallu quitter les États-Unis pour comprendre vraiment ce que cela signifiait. Si le World Wide Web a été inventé à Genève, dans les laboratoires de recherche du CERN, en 1989, les divers modes d'accès à internet sont aussi américain que le base-ball, ce qui confère un avantage déterminant aux services de renseignement des États-Unis. Qu'ils s'agisse des câbles, de satellites, des serveurs ou des tours, l'infrastructure d'Internet est à ce point contrôlé par les américains que 90 % du trafic mondial s'effectue grâce à un ensemble de technologies développées, possédées et/ou mises en œuvre par les autorités et les grandes entreprises américaines, pour la plupart situées aux États-Unis… (…) les États-Unis conservent l'hégémonie en la matière et qu'ils contrôlent l'interrupteur à même de connecter ou de déconnecter pratiquement le monde entier à volonté.*
Il n'y a pas que l'infrastructure d'Internet qui soit essentiellement américaine, il y a aussi les logiciels (Microsoft, Google, Oracle), le hardware (Hewlett Packard, Apple, Dell) et tout le reste, depuis les puces (Intel, Qualcomm), les routeurs et les modems (Cisco, Juniper) jusqu'aux services et aux plateformes web qui permettent d'échanger des e-mails, d'aller sur les réseaux sociaux et stocker des données en ligne (Google, Facebook et Amazon, le dernier étant structurellement le plus important , même si ça ne se voit pas, car il fournit le service de cloud au gouvernement américain est à la moitié d'Internet). Ces entreprises font peut-être dans certains cas fabriquer leur matériel en Chine, par exemple, elles n'en demeurent pas moins américaines et sont donc assujetties à la législation en vigueur aux États-Unis. L'ennui, c'est qu'elles sont aussi tributaires de décision politiques américaines secrètes qui détournent la loi et autorisent le pouvoir à surveiller pratiquement n'importe quel homme, femme ou enfant s'étant déjà servi d'un ordinateur ou d'un téléphone.
Étant donné le caractère américain de l'infrastructure des communications mondiales, il était prévisible que le gouvernement se livrerait à la surveillance de masse. »

p. 192-194
« *juste après les attentats du 11 sept. 2001, le Président George W. Bush avait autorisé la NSA à multiplier les opérations de surveillance. Celle qui a entraîné le plus de polémique visait à enregistrer les conversations téléphoniques sans avoir besoin d'un mandat délivré par la justice. Elle figurait en bonne place dans le Programme de Surveillance du Président, PSP, ainsi que l'a révélé le New York Times en 2005 après avoir été contacté par de courageux lanceurs d'alerte de la NSA et du ministère de la justice*… (…) …
Les révélations du New York Times déclenchèrent un véritable tollé et l'Union américaine pour les libertés civiles avait saisi la justice et contesté devant les tribunaux la constitutionnalité de telles dispositions. L'administration Bush avait alors déclaré que ce programme prendrait fin en 2007 mais c'était une vaste blague. Le Congrès a passé en effet les deux dernières années du mandant de George W. Bush à voter des lois qui justifiaient rétroactivement le PSP et dédouanaient les entreprises des télécommunications et les fournisseurs d'accès à Internet impliqués. Cette législation – le Protect America Act de 2007 sur la protection de l'Amérique et le FISA Amendment Acts de 2008 – employait délibérément une langage équivoque pour faire croire aux Américains que leurs communications n'étaient pas visées, alors même que la loi élargissait le champ d'action d'application du PSP. Non seulement la NSA interceptait les communications venant de l'étranger mais elle pouvait désormais intercepter les conversations téléphoniques et les e-mails émanant de l'intérieur du pays.
Telles sont du moins les conclusions que j'ai tirées de la lecture du résumé de la situation rendu public par le gouvernement en juillet 2009, l'été au cours duquel je me penchais sur les cyber-capacités chinoises. Ce document sobrement intitulé « Rapport public sur le Programme de Surveillance du Président »… (…) … *Je me souviens avoir tout de suite été frappé par son ton curieux qui semblait s'insurger devant les protestations, et par le fait qu'il prenait quelques libertés avec le langage*… (…) … *Une chose encore m'a interloqué dans ce rapport. On y multipliait en effet les références aux « Autres Opérations de Renseignement »*… (…) … *Il va de soi que ces références n'expliquaient pas en quoi consistaient ces « opérations », mais par déduction, j'ai compris qu'il s'agissait de se livre à des activités de surveillance intérieures sans mandat*… (…) *Voilà qui m'a amené à rechercher la version classifiée de ce rapport, et ne pas la trouver ne m'a pas rassuré.* »
p. 196-198
« *Ce n'est que plus tard, alors que j'avais depuis longtemps oublié ce mystérieux rapport confidentiel, qu'il a atterri sur mon bureau… (…) il demeurait inaccessible aux dirigeants des services secrets eux-mêmes. On l'avait classé parmi les documents relevant des « informations soumises à un contrôle exceptionnel »*… (…)

seules quelques dizaines d'individus dans le monde étaient autorisées à en prendre connaissance. Je ne faisais assurément pas partie du lot et c'est à la suite d'une erreur que j'en ai pris connaissance… (…)
D'ordinaire, je me contentais d'y jeter un coup d'œil mais cette fois, il m'a suffi de l'ouvrir et de découvrir son titre pour savoir que je le lirais jusqu'au bout.
Il contenait tout ce qui manquait dans la version non classifiée, tout ce dont n'avaient pas parlé les journalistes, tout ce que la procédure judiciaire, que j'avais suivie, avait nié : un exposé détaillé des programmes de surveillance les plus secrets de la NSA, ainsi que la liste des directives qu'elle avait données et l'exposé de la ligne stratégique adoptée par le ministère de la justice pour contourner la loi et violer la constitution américaine… (…) *… Et il décrivait les manœuvres si foncièrement criminelles qu'aucun gouvernement ne pouvait le rendre public sans l'expurger au préalable.*
Quelque chose m'a immédiatement sauté aux yeux : il était évident que la version non classifiée que j'avais lue n'était pas une révision de la version classifiée, comme c'était le cas habituellement. C'était un texte complètement différent, un tissu de mensonges quand on le comparait au rapport classifié. La duplicité était proprement stupéfiante… (…)
Au lieu d'évoquer l'interception et l'enregistrement ciblés de communications, le rapport évoquait une « collecte de grande ampleur », ce qui est un euphémisme utilisé par l'agence pour désigner la surveillance de masse. Et tandis que la version déclassifiée passait sous silence ce changement, agitant l'épouvantail du terrorisme pour mieux préconiser l'adoption de mesures de surveillance élargies, la version classifiée était très explicite à ce sujet et n'y voyait qu'une conséquence logique des progrès technologiques… (…)
En substance la NSA affirmait que la législation américaine avait été dépassée par l'accroissement du volume et de la rapidité des échanges – aucun tribunal, même secret, ne pouvait suivre le rythme et délivrer un temps voulu assez de mandats – et qu'à un monde globalisé devait répondre une agence de renseignement véritablement mondiale.
Dans la logique de la NSA, tous ces éléments soulignaient la nécessité d'une collecte de grande ampleur des communications Internet.
Le nom de code de cette collecte de grande ampleur était indiqué par le « gros mot » [mots qui identifient des fichiers à supprimer de la plupart des disques durs] *qui apparaissait dans mon système : « STLW », l'abréviation de STELLARWIND (« vent solaire »). Il s'est avéré que c'était la seule mesure d'importance figurant dans le PSP qui avait continué à être appliquée est s'était même renforcée une fois que le reste du programme avait été rendu public dans la presse.*
STELLLARWIND était ce qu'il y avait de plus confidentiel dans ce rapport classifié. C'était en fait le secret le mieux gardé de la NSA, que le statut « sensible » du rapport visait à protéger. L'existence même de ce programme attestait que la mission de la NSA s'était transformée : l'informatique, destinée à l'origine à protéger les États-Unis, était désormais utilisée pour contrôler le pays, redéfinissant les communications Internet privées des citoyens comme du renseignement électromagnétique. »
p. 199.
« *STELLAWIND collectait des renseignements depuis l'entrée en vigueur du PSP en 2001 mais c'est en 2004 – lorsque les agents du ministère de la Justice rechignèrent à poursuivre l'initiative – que l'administration Bush tenta de la légitimer a posteriori en donnant un sens différent à quelques mots simples tels qu' « acquérir » ou « obtenir ». A en croire ce rapport, le gouvernement estimait que la NSA pouvait enregistrer autant de communications qu'elle voulait sans mandat, car elle n'avait jamais fait qu'acquérir ou obtenir ces informations, au sens légal, lorsqu'elle les « recherchait » dans ses bases de données puis les « récupérait »…*
Cette tartufferie lexicale m'agaçait d'autant plus que j'avais parfaitement conscience que la NSA désirait conserver le maximum de données le plus longtemps possible, voire indéfiniment. Si les enregistrements des communications ne pouvaient être considérés comme « obtenus » qu'une fois qu'ils avaient été utilisés, ils pouvaient, dans le cas inverse, demeurer « non obtenus » tout en étant stockés ou archivés à jamais, en attente d'une manipulation future.
En accordant un sens différent aux termes « acquérir » et « obtenir » - depuis l'instant où ces données intégraient une banque de données jusqu'à celui où un individu (ou plus vraisemblablement un algorithme) lançait une recherche dans la base où se trouvait une occurrence - , le gouvernement américain créait une agence éternelle de maintient de l'ordre. Il pouvait à tout moment fouiller dans les communications passées de tous (et les communications de chacun d'entre nous contiennent des preuves de quelque chose). A tout moment, et cela jusqu'à la fin des temps, une nouvelle administration ou un autre patron dévoyé de la NSA

serait en mesure de surveiller toute personne ayant un ordinateur ou un portable, de connaître son identité, sa localisation géographique ainsi que son activité, présente et passée.
Comme la plupart des gens, je préfère parler de « surveillance de masse » que de « collecte de grande ampleur », l'expression utilisée par le gouvernement, car cette dernière brouille l'image de la NSA.
« Collecte de grande ampleur » fait penser à un bureau de poste débordant d'activité ou au ramassage des ordures ménagères plutôt qu'à un effort historique visant à intercepter – et à enregistrer clandestinement – l'ensemble des communications numériques. »

p. 200-201
« *Mais hélas la teneur de nos communications en dit rarement autant sur nous que d'autres éléments qui restent tacites. Je veux parler des informations qui ne sont pas dites ni écrites mais qui permettent néanmoins de révéler un contexte plus large et des modèles de comportements.*
La NSA appelle cela des « métadonnées », le préfixe « méta » traditionnellement par « au dessus » ou « au delà », est ici utilisé dans le sens d'« à propos » ; des données à propos d'autre données… (…) *… Les métadonnées d'un e-mail peuvent indiquer le genre d'ordinateur utilisé, le nom de son propriétaire, le lieu depuis lequel il a été envoyé, qui l'a reçu, quand il a été expédié et quand il a été reçu, qui l'a éventuellement lu en dehors de son auteur et de son destinataire, etc. Les métadonnées peuvent permettre à celui qui vous souveille de connaître l'endroit où vous avez passé la nuit et à quelle heure vous vous êtes réveillé ce matin là. Elles permettent de retracer ce que fut votre parcours dans la journée, combien de temps vous avez passé dans chaque endroit visité et avec qui vous avez été en contact…* (…) *… Voilà pourquoi il ne faut pas envisager les métadonnées comme des abstractions inoffensives mais comme l'essence même du contenu : elles sont précisément la première source d'information exigée par celui qui vous surveille…* (…) *… vous ne contrôlez pas, ou à peine, les métadonnées que vous générez automatiquement. C'est une machine qui les fabrique sans vous demander votre participation ni votre autorisation, et c'est aussi une machine qui les recueille, les archive et les analyse…* (…) *…* l*es agences de renseignement s'intéressent bien plus à ces dernières -, qui leur permettent d'avoir à la fois une vue d'ensemble en analysant les données à grande échelle, et une vue détaillée en réalisant les cartographies précises, les chronologies et les synthèses associatives de la vie d'un individu, à partir desquelles ils extrapolent des prédictions comportementales.* »
p. 203.
« *Le portable qu me permettait de m'orienter et me corrigeait quand je me trompais de direction, qui me traduisait les panneaux indicateurs et me donnait les horaires des bus et des trains, veillait également à ce que mes patrons connaissent mes moindres faits et gestes. Mon téléphone leur indiquait quand je m'étais trouvé à tel endroit sans même que j'ai eu besoin de le toucher ou de le sortir de ma poche.* »

p. 215-217.
« *Tout comme la surveillance gouvernementale assujettissait les citoyens, qui se trouvaient à la merci du pouvoir étatique, la surveillance des grandes entreprises transformait le consommateur en produit que ces mêmes corporations vendaient à des homologues, des courtiers de données et des annonceurs.*
Pendant ce temps, toutes les grosses sociétés d'informatique, y compris Dell, lançaient des versions grand public de ce sur quoi je travaillais pour le compte de la CIA, à savoir le cloud. (A vrai dire, Dell avait même essayé de déposer quatre ans plus tôt l'expression « cloud computing », sans succès). Je n'en revenais pas de voir les gens y souscrire allègrement, tellement excités de se dire que leurs photos, leurs vidéos, leur musique et leur livres numériques allaient être dupliqués et que tout le monde pourrait y avoir accès qu'ils ne se demandaient jamais vraiment pour quelle raison ce mode de stockage pratique et si sophistiqué était « gratuit » ou du moins « bon marché »…. (…) …
« *Ce cloud, Dell le vendait à la CIA ou bien aidait Amazon, Apple et Google à le fourguer à leurs utilisateurs…* (…) *… Ce « nuage » qui flottait au dessus de la mélée était blanc, cotonneux et pacifique…* »
p. 216.
« *Dell, comme les plus importantes sociétés privées qui s'appuyaient sur le clould (Amazon, Apple et Google), voyait son essor comme un nouvel âge informatique. Mais sur le plan conceptuel au moins, il marquait un retour au vieux système des débuts de l'informatique, qui reposait sur la dépendance des utilisateurs à une unités centrale puissante que seule une élite de cadres et de professionnels était capable d'entretenir…* (…)
vos données ne vous appartiennent plus vraiment, elles sont contrôlées par des entreprises qui peuvent s'en servir pour faire pratiquement n'importe quoi… (…) *… Choisir de stocker ses données en ligne revient*

souvent à en céder les droits. Les entreprises du cloud sont libres de de garder ou de supprimer les données qu'on leur confie suivant que ça leur plaît ou non… (…) *… Si certaines de vos données les dérangent ou contreviennent aux termes du contrat de service, les entreprises du cloud peuvent fermer notre compte et refuser de nous laisser consulter nos données tout en conservant un double dans leurs archives, qui leur est ensuite possible de remettre aux autorités sans nous avertir ni nous demander notre autorisation. »*

p. 218.
« *Le données des utilisateurs généraient d'énormes profits pour les entreprises et étaient pillées sans complexe par le gouvernement. Je ne pense pas m'être jamais senti si impuissant.* »
« *Aux États-Unis les lois fondamentales…* (…) *… c'est l'une des caractéristiques essentielles de la démocratie…* (…) *…. L'une des plus importantes de ces restrictions concerne l'interdiction aux forces de l'ordre de surveiller les gens lorsqu'ils se trouvent sur leur propriété et de s'emparer d'enregistrement privés sans disposer d'un mandat.* »
p. 369.
« *… article 12 de la Déclaration universelle des droits de l'homme des Nations Unies, qui date de 1948 et qui stipule : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.* »

p. 248.
« *Un ordre de la cour FISA, la cour de surveillance du renseignement étranger des États-Unis, était à mes yeux bien plus révélateur : il s'agissait d'une requête juridique adressée à une entre prise privée sur ses clients. Ce type d'ordre était théoriquement émis sous l'autorité de la législation publique ; pourtant leur contenu, voire leur existence était classé « top secret ». En vertu de la section 215 du Patriot Act, également connue sous le nom de disposition sur les « registres commerciaux », le gouvernement était autorisé à obtenir un ordre de la cours FISA contraignant des « parties tierces » à produire « tout élémennt tangible » susceptible d'être « pertinent » pour le renseignement extérieur et la lutte contre le terrorisme. Mais comme le rendait parfaitement clair l'ordre de la cour en question, la NSA avait secrètement interprété cette autorisation comme une licence pour collecter toutes les métadonnées des communications téléphoniques transitant par des opérateurs américains, comme Verizon ou AT&T, le tout « sur une base quotidienne continue ». Ceci incluait bien sûr l'enregistrement de communications téléphoniques entre citoyens américains, une pratique par définition anticonstitutionnelle.*
De plus, la section 702 du FISA Amendments Acts autorise la communauté du renseignement à cibler tout étranger à l'extérieur des États-Unis dont on estime qu'il exise une probabilité suffisante pour qu'il communique une « information relevant du renseignement étranger », ce qu correspond à une vaste catégorie de cibles potentielles incluant journalistes, employés d'entreprises, chercheurs, travailleurs humanitaires, ainsi que d'innombrables autres innocents. C'est cette législation qui a permis à la NASA de justifier ses deux principales méthodes de surveillance d'Internet, à savoir Upstream Collection et le programm PRISM.
PRISM a permis à la NSA de collecter régulièrement des données auprès de Microsoft, Yahoo !, Google, Facebook, Paltalk, You Tube, Skype, AOL et Apple, dont des e-mails, des photos, des chats audio et vidéo, des historiques de navigation, des historiques de recherches et tout autre donnée susceptible d'être abritées sur le cloud, transformant ces entreprises en des complices tout à fait conscients de ce qu'ils faisaient.
Upstream Collection, quant à lui, était potentiellement encore plus invasif. Il permettait la capture régulière de données directement sur les infrastructures Internet du secteur privé – les interrupteurs et les routeurs qui aiguillaient le trafic internet mondial via les satellites en orbites et les câbles de fibre optique parcourant le fond des océans. Cette collecte était opérée par une unité de la NSA appelée Special Sources Operations, qui avait construit un équipement secret de mise sur écoute et l'avait installé dans les locaux des fournisseurs d'accès à Internet partout dans le monde.
Pris ensemble, PRISM (qui collecte des données sur les serveurs des fournisseurs de services) et Upstream Collection (qui collecte directement des données sur les infrastructures d'Internet) garantissaient que toutes les informations du monde, qu'elles soient stockées ou en transit, était bien « surveillables »). »

p. 250.

« *… les technologies derrière Upstream Collection existaient bel et bien. J'ai pu constater que ces outils étaient les éléments les plus invasifs de tout le système de surveillance de masse de la NSA, ne serait-ce que parce qu'ils sont les plus proche de l'utilisateur – c'est-à-dire les plus proches de la personne en train d'être surveillée. Imaginez-vous assis devant un ordinateur, alors que vous êtes sur le point de vous rendre sur un site web. Vous ouvrez votre navigateur, tapez un URL, et appuyer su la touche « Entrée ». L'URL est une requête, et cette requête est envoyée vers son serveur de destination. Mais quelque part au cours de son voyage, avant que la requête ne parvienne à son serveur, elle devra passer à travers TURBULENCE, l'une des armes les plus puissantes de la NSA.*
Plus spécifiquement, votre requête passera par plusieurs serveurs noirs empilés les uns sur les autres, d'à peu près la taille d'une bibliothèque à quatre rayonnages. Ces serveurs sont installés dans des salles spéciales au sein de bâtiments appartenant aux plus grands opérateurs télécoms privé dans des pays alliés, ainsi que dans des ambassades et des bases militaires américaines. Ils utilisent deux outils capitaux. Le premier, TURMOIL, gère la « collecte passive ». Le second TURBINE, est responsable de la « collecte active » - au sens ou elle manipule activement les données de l'utilisateur.
Vous pouvez imaginer TURMOIL comme un garde posté devant un par-feu invisible à travers lequel passe tout le trafic Internet. Quand votre requête arrive, il vérifie ses métadonnées pour voir si elles possèdent l'un des critères indiquant que la requête doit être examinée de plus près. Ces critères sont du ressort arbitraire de la NSA, et relèvent de tout ce que l'agence considère comme suspect : une adresse mai, un numéro de carte de crédit ou un numéro de téléphone particulier ; l'origine ou la destination géographique de votre activité Internet ; ou bien juste certains mots-clés comme « proxy anonyme » ou « manif ».
Si TURMOIL décide que votre navigation est suspecte, il transmet l'info à TURBINE, qui redirige votre requête vers les serveurs de la NSA ; la-bas, des algorithmes décident quel programme – quel logiciel malveillant, ou malware – de l'agence va être utilisé contre vous. Ce choix est aussi bien fondé sur le type de site que vous vous apprêtez à visiter que sur vote connexion Internet ou les softwares qu'utilise votre ordinateur. Les programmes choisis sont renvoyés à TURBINE (par des programmes de la suite QUANTUM, si vous vous posez la question), qui les injecte dans le trafic et vous les refile en même temps que le site web que vous cherchiez à visiter. Et voilà le résultat : vous avez eu ce que vous vouliez, avec la surveillance dont vous ne vouliez pas, le tout en moins de 686 millisecondes. Et complètement à votre insu.
Une fois que les programmes sont sur votre ordinateur, la NSA n'a plus seulement accès à vos métadonnées mais également à toutes vos données. Désormais votre vie numérique lui appartient entièrement. »

p. 255, parlant de la Constitution en vigueur des États-Unis d'Amérique :
« *Les amendements IV à VIII avaient tous été délibérément est soigneusement conçus pour entraver et diminuer la capacité du gouvernement à exercer son pouvoir et organiser sa surveillance.*
*C'est tout particulièrement vrai du Iv*è *amendement, qui protège les individus de leurs biens de la surveillance du gouvernement : « Le droit des citoyens d'être garantis dans leur personne, domicile, papiers et effets, contre les perquisitions est saisies non motivées ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse, corroborées par serment ou affirmation, si sans qu'il décrive particulièrement le lieu à fouiller et les personnes ou les choses à choisir.* »
p. 256. « *Au cours des siècles qui nous séparent du premier jour de la Constitution, nos clouds, nos ordinateurs et nos téléphones sont devenus nos maisons, aussi personnels et intimes que nos maisons physiques. Si vous n'êtes pas d'accord, alors répondez à cette simple question : est-ce que vous préféreriez laisser vos collègues traîner seuls dans votre maison pendant une heure ou leur donner accès à votre téléphone ne serait-ce que dix minutes ?* » (….)
« *… la NSA maintenait que dans la mesure où vous aviez déjà « partagé » les données contenues dans votre téléphone avec un « tiers » - votre opérateur téléphoniques -, vous aviez renoncé à tout droit constitutionnel à la vie privée que vous aviez pu avoir dans le passé.* »
p. 257. « *Si les mécanismes de surveillance constitutionnelle avaient correctement fonctionné, cette interprétation pour le moins radicale du IV*è *amendement – qui soutient que l'acte même d'utiliser des technologies modernes équivaut à renoncer à ses droits à la vie privée – aurait été rejetée par le Congrès est les cours de justice.* »

p. 259.

« *L'examen de la constitutionnalité de cette infrastructure fut donc confié, selon les mots même de l'American Civil Liberties Union (l'ACLU, l'Union américaine pour les libertés civiles), à une cour secrète chargée d'autoriser des programmes secrets tout en réinterprétant secrètement la loi fédérale.*
Quand des associations de la société civile comme l'ACLU tentèrent de remettre en cause les activités de la NSA devant les cours fédérales ordinaires et publiques, il se produisit quelque chose d'étrange. Le gouvernement ne se défendit pas en se fondant sur l'idée que ses activités se surveillance étaient légales ou constitutionnelles. Il préféra déclarer que l'ACLU et ceux que l'association représentait n'avaient aucun droit d'attaquer le gouvernement en justice dans la mesure où l'ACLU n'était pas capable de prouver que ses clients avaient effectivement fait l'objet d'une surveillance. De plus, l'ACLU ne pouvait utiliser le contentieux pour obtenir les preuves d'une surveillance car l'existence (ou la non-existence) d'un telle preuve était un « secret d'État », et que les fuites dans la presse ne comptaient pas. Autrement dit, la cour ne pouvait prendre en compte une information qui était pourtant publique puisqu'elle avait été publiée dans les médias ; elle pouvait seulement apprécier les informations que le gouvernement avait officiellement confirmé être connues du public. Cet argument de la classification signifiait que ni l'ACLU ni personne d'autrte ne serait jamais en mesure d'attaquer le gouvernement sur ces questions devant une cour de justice non secrète. J'ai été particulièrement dégoûté quand, en février 2013, la cour suprême a décidé par 5 voix contre 4 d'accepter le raisonnement du gouvernement et a, sur cette base, débouté l'action en justice intentée par l'ACLU et Amnesty International afin de remettre en cause la surveillance de masse sans même considérer la question de la légalité des activités de la NSA. »

p. 260.
« *Je me suis rendu compte que j'avais été terriblement naïf de croire que la Cour suprême, le Congrès ou le président Obama, en cherchant à rompre avec le gouvernement de George W. Bush, accepterait de tenir la communauté du renseignement pour juridiquement responsable de quoi que ce soit. Il était temps d'admettre que cette communauté se croyait au dessus des lois, et vu à quel point le système était vérolé, qu'elle avait raison de le croire.* »

p. 262.
« *… le Congrès… en 1778… et à l'unanimité, vota la première loi de protection des lanceurs d'alerte. Cette loi déclarait qu'il était du « devoir de toutes les personnes au service des États-Unis, ainsi que de tous ses habitants, de transmettre le plus tôt possible, toute information au Congrès ou à toute autre autorité adaptée concernant toute fraude, faute ou délit commis par tout officier ou personne de service de ces États ont ils auraient eu connaissance. ». Cette loi m'a donné de l'espoir, et c'est toujours le cas.* »
p. 263. « Peu, voir aucun de mes supérieurs de la communauté du renseignement, n'auraient été prêts à sacrifier leur carrière au nom de ces mêmes principes pour lesquels le personnel militaire sacrifiait régulièrement sa vie. »

p. 266.
« *La communauté du renseignement aime bien annoncer ses « succès » indépendamment de la classification de ces informations et indépendamment des conséquences que peut avoir leur divulgation. Ce point a été particulièrement frappant lors de la fuite liée à l'assassinat extra-judiciaire, au Yémen, de l'imam extrémiste né aux États-Unis Anwar al-Awlaqi. En ne cessant de transmettre des informations sur son attaque de drone contre contre al-Awlaqi au Washington Post et au New York Times, l'administration Obama admettait tacitement non seulement l'existence du programme de drones de la CIA mais également celle de la « disposition Matrix », soit la liste des « hommes à abattre », tous deux officiellement top secrets. En outre le gouvernement confirmait implicitement qu'il commanditait non seulement des assassinats ciblés mais, qui plus est, des assassinats ciblés de citoyens américains. Ces fuites, divulguées avec toute la coordination que nécessite une campagne médiatique, constituait la démonstration choquante du deux poids deux mesures avec lequel l'État aborde la question du secret : un sceau doit être maintenu afin que le gouvernement puisse agir en toute impunité, mais il peut être brisé pour peu que le gouvernement ait besoin de s'attribuer un mérite.* »

p. 274.
« *WikiLeaks collaborait régulièrement avec les plus grands journaux internationaux, comme The Guardian, The New York Times, Der Spiegel, Le Monde ou El País, pour publier les documents que lui avaient fournis ses sources. Le travail qu'ont accompli ces organes de presse de 2010 à 2011 m'a fait penser que la plus*

grande valeur de WikiLeaks reposait dans sa capacité à jouer les intermédiaires entre les journalistes et les sources et à faire office de pare-feu protégeant l'anonymat de ces dernières.
Les pratiques de WikiLeaks ont changé après la publication des révèlations de la soldate américaine Chelsea Manning – une multitude de « journaux internes » de l'armée américaine relatifs à la guerre en Irak et à la guerre en Afghanistan, des informations sur les prisonniers de Guantanamo, ainsi que des centaines de milliers de câbles diplomatiques américains. A la suite des représailles du gouvernement et de la controverse suscitée dans les médias par l'éditorialisation qu'avait fait WikiLeaks du matériau transmis par Manning, Wikileaks avait décidé de changer son fusil d'épaule et de publier les futures fuites telles qu'elles étaient reçues : vierges de tout travail éditorial. Ce passage à une transparence totale signifiait que publier sur WikiLeaks ne correspondait plus à mes besoins… … je savais que l'histoire racontée par ces documents de la NSA, celle d'un système global de surveillance de masse déployé dans le plus grand secret, était difficile à comprendre. »

p. 277.
«*… l'annonce par la NSA de la construction d'un immense centre de stockage et de traitement de données à Bluffdale, dans l'Utah. L'agence l'avait appelé le Massive Data Repository (« Entrepôt de données en masse », jusqu'à ce que quelqu'un d'un peu plus doué que les autres en relations publiques se rende compte que ce nom serait difficile à expliquer s'il fuitait, si bien que le centre a été renommé Mission Data Repository (« Entrepôt de données de mission ») - conserver le même acronyme permettait d'éviter de remplacer tous les slides de présentation. Il était prévu que le MDR fasse environ 39 500 m² et soit rempli de serveurs. Il pouvait héberger une quantité phénoménale de données, en gros une sorte d'histoire en perpétuelle évolution des faits et gestes à l'échelle de la planète, dans la mesure où la vie peut-être modélisée en connectant des paiements à des individus, des individus à des téléphones, des téléphones à des appels et des appels à des réseaux...* »
p. 278. « *Personne n'a posé les questions qui me semblaient les plus évidentes : pourquoi une agence gouvernementale, sans même parler d'une agence de renseignement, aurait-elle besoin d'autant d'espace ? Quelles données et en quelle quantité avait-ils l'intention d'y stocker ? Pour combien de temps ? Il n'existait tout simplement aucune raison valable de construire un monstre doté de telles spécifications à moins de projeter de tout stocker jusqu'à la fin des temps. Selon moi, c'était là le corps du délit – la confirmation, claire comme le jour, qu'un crime était commis au sein d'un gigantesque bunker de béton entouré de fil de fer barbelé et de miradors, qui pompait autant d'électricité qu'il n'en faut pour alimenter une ville entière et disposait de son propre réseau de distribution électrique en plein milieu du désert de l'Utah. Et personne n'y prêtait la moindre attention.* »

p. 277-78.
«*… année suivante, en mars 2013… Clapper avait nié que la NSA collectait en masse les données des citoyens américains… En revanche aucune publication mainstream n'avait couvert l'une des rares apparitions publiques d'Ira « Gus » Hunt, le directeur de la technologie de la CIA. Je connaissais un peu Gus depuis mon passage chez Dell avec la CIA. Il était l'un de nos meilleurs clients…. … et les conférences les plus importantes, comme celle de Gus, étaient visibles gratuitement et en direct en streaming.*
Il était l'un des intervenant… un évènement consacré à la technologie civile à New York… L'agence avait…
… signer un contrat de 600 millions de dollars avec Amazon pour le développement et la gestion de son cloud pour une durée de 10 ans
… parler dans un costard tout frippé des ambitions et des capacités de l'agence à une foule de civils sans accréditation – et via Internet, au monde entier, qui n'avait pas plus d'accréditation. Plus sa présentation avançait, entre mauvaises blagues et manipulation bouffonne de PowerPoint, plus mon incrédulité grandissait.
« *A la CIA, a-t-il dit, nous essayons de tout collecter et de tout conserver pour toujours. » Comme si ça n'était pas assez clair, il a rajouté : « Nous sommes désormais quasiment en mesure de traiter toute les informations crées par les humains » - je précise que ces Gus lui-même qui soulignait…* (…)
Gus a dit aux journalistes que l'agence pouvait pister leurs smart-phones même quand ils étaient éteints, qu'elle était capable de surveiller toutes leurs communications. Rappelez-vous : il s'agissait d'une assemblée de journaliste américains. Et le « pouvait pister » a sonné comme un « le fait » et « le fera ». Il pérorait d'une manière extrêmement brouillonne, du moins pour un ponte de la CIA : « La technologie va trop vite pour le gouvernement ou pour la loi. Elle va trop vite pour vous. La seule question que vous devez

vous poser c'est quels sont vos droits, et qui possède vos données. ». J'étais sidéré. N'importe quelle personne moins gradée qui aurait prononcé un discours pareil se serait retrouvée derrière les barreaux avant la fin de la journées.
La confession de Gus n'a été couverte que par le Huffington Post. Mais la performance en tant que telle est encore disponible sur You Tube à l'heure où j'écris ces lignes, soit six ans plus tard. La dernière fois que j'ai vérifié, la vidéo avait 313 vues – dont une dizaine de mon fait. »

p. 299.
« *Les derniers jours de 2012 ont été marqués par de sinistres nouvelles. Les derniers remparts légaux qui interdisaient la surveillance de masse par certains des membres les plus importants des « Five Eyes »* [USA-GB-Canada-Australie-NZ qui s'échangent les données] *étaient en train de tomber. Les gouvernements australiens et britanniques proposaient tous deux des législations pour rendre obligatoire l'enregistrement des métadonnées téléphoniques et d'Internet. C'était la première fois que des gouvernements en théorie démocratiques confessaient publiquement leur ambition de construire une sorte de machine à remonter le temps de la surveillance qui leur permettrait, grâce à la technologie, de revenir sur les évènements de la vie de n'importe quel individu, et ce jusqu'à plusieurs mois voir des années en arrière. Ces tentatives ont définitivement marqué, du moins dans mon esprit, le passage d'un monde occidental créateur et défenseur d'un internet libre à un monde occidental ennemi et destructeur de ce même Internet.* »

p. 308.
« *Le programme qui rendait possible cet accès était appelé XKEYSCORE, que l'on pourrait décrire comme un moteur de recherche permettant à l'analyste de chercher dans tous les enregistrements de votre vie. Imaginez une sorte de Google qui, au lieu de montrer des pages de l'Internet public, proposerait des résultats issus de vos e-mail privés, de vos chats privés, de vos fichiers privés, etc.…* »
p. 311-12.
« *C'était, pour dire les choses simplement, ce que j'ai pu voir de plus proche de la science-fiction dans la science elle-même : une interface permettant de taper l'adresse, le numéro de téléphone ou l'adresse IP d'à peu près n'importe qui et de se plonger dans l'histoire récente de son activité en ligne. Dans certains cas, vous pouviez même visualiser des enregistrements de ses sessions en ligne passées, si bien que vous ne regardiez plus votre écran mais le sien, avec tout ce qui traînait sur son bureau. Vous accédiez à ses e-mails, son historique de navigation, son historique de recherche, ses posts sur les réseaux sociaux, etc. Vous pouviez activer des notifications pour être averti à chaque fois qu'une personne ou une machine qui vous intéressaient devenait active sur internet. Et vous pouviez regarder dans les paquets de données d'Internet pour voir apparaître les recherches d'un individu lettre par lettre, dans la mesure où de très nombreux sites transmettaient chaque caractère au fur et à mesure qu'ils étaient tapés. C'était comme regarder un « complément automatique » : les lettres et les mots apparaissaient un par un sur l'écran, sauf que l'intelligence à l'œuvre n'était pas artificielle mais bien humaine – c'était un « complément humain ».*
Les semaines passées à Fort Meade et mon court passage chez Booz [Hallen] *lors de mon retour à Hawaï ont été les seules fois où j'ai vu de mes yeux les abus en train d'être commis, abus dont je connaissais auparavant l'existence que par ma lecture de la documentation interne. Constater ces abus m'a fait réaliser combien ma position au niveau des systèmes m'avait éloigné de l'impact réel de ces programmes et m'avait isolé du niveau zéro du dommage immédiat. Je ne pouvais qu'imaginer alors le degré d'éloignement de la direction de l'agence ou, tant qu'on y était, du président des États-Unis.* »
p. 313. « *Cette tendance est à l'origine de la pratique connue sous le nom de LOVEINT… les analystes utilisaient les programmes de l'agence pour surveiller leurs partenaires amoureux ou leurs ex – lire leurs e-mails, écouter leur conversations téléphoniques et les traquer sur la toile. Les employés de la NSA savaient que seuls les analystes vraiment stupides s'étaient fait prendre la main dans le sac. Même si la loi déclarait que quiconque exerçant une surveillance de quelque type que ce soit à des fins personnelles pouvait passer plus de dix ans derrière des barreaux, personne, de toute l'histoire de l'agence n'avait jamais passer ne serait-ce qu'une journée en prison pour ce crime. Les analystes savaient que le gouvernement ne les poursuivraient jamais publiquement en justice : il paraît quelque peu compliqué d'accuser quelqu'un d'avoir abusé de votre système secret de surveillance de masse sans accepter de reconnaître l'existence du système lui-même.* »
p. 314.
« *Une chose que vous compreniez très rapidement en utilisant XKEYSCORE, c'est que quasiment toutes les personnes dans le monde qui se trouve en ligne ont au moins deux choses en commun : elles ont toutes maté*

du porno à un moment ou à un autre et elles ont toutes stocké des vidéos et des photos de leur famille. C'est vrai pour tout le monde, indépendamment de votre genre, de votre race ou de votre âge – depuis le plus vicieux des terroristes jusqu'à la plus adorables des personnes âgées, qui peut d'ailleurs très bien être le grand-parent, le parent ou le cousin du plus vicieux des terroristes.
Ce sont les trucs de famille qui me touchaient le plus. Je me souviens en particulier d'un gosse, un petit garçon en Indonésie. Techniquement, je n'aurais pas du m'intéresser à ce petit garçon mais je l'ai fait, tout simplement parce que mon employeur s'intéressait à son père. J'avais lu tout le dossier partagé de la cible qu'avait constitué un annaliste « persona », c'est-à-dire quelqu'un qui passait le plus clair de son temps à passer au crible des artefacts tels que des historiques de discussions et de messages Gmail ou Facebook, plutôt que d'analyser le trafic Internet plus complexe et plus obscur, généralement généré par des hackers, comme le faisaient les analystes infrastructure.
Le père du petit garçon était, comme le mien, ingénieur – mais contrairement à mon père, il n'était pas affilié au gouvernement ou à l'armée. C'était juste un universitaire que s'était retrouvé dans la nasse de la surveillance. Je n'arrive même pas à me souvenir pourquoi et comment il avait attiré l'attention de l'agence, à part le fait qu'il avait postulé pour faire de la recherche dans une université en Iran. Les raisons à l'origine des soupçons était généralement fort peu documentés, voire pas du tout, et les connexions pouvaient être incroyablement ténues - « soupçonné d'être potentiellement lié à », suivi du nom d'une organisation internationale qui pouvait être n'importe quoi, depuis un organe de normalisation des télécommunications jusqu'à l'UNICEF en passant par des organisations que l'on pourrait effectivement considérer comme un menace.
Le flux du trafic Internet avait été passé au tamis et des sélections de communications de l'homme avaient été rassemblées dans un dossier – ici, c'était la copie fatale du CV qu'il avait envoyé à l'université suspecte, là ses textes, là, l'historique de son navigateur, et là, toute sa correspondance de la semaine précédente, à la fois ce qu'il avait envoyé et ce qu'il avait reçu, le tout associé à des adresses IP. On trouvait aussi les coordonnées d'un « gardiennage virtuel » que l'analyste avait placé autour de l'homme afin d'être averti s'il s'aventurait trop loin de chez lui ou se rendait à la fameuse université pour son entretien d'embauche. Ses photographies étaient également rassemblées, ainsi qu'une vidéo. Il était assis devant son ordinateur, exactement comme je l'étais en ce moment même. Sauf que sur ses genoux se trouvait un tout petit garçon qui portait une couche.
Le père essayait de lire quelque chose mais le gosse passait son temps à gigoter, à appuyer sur les touches du clavier et à glousser. Le micro interne de l'ordinateur captait son petit rire et j'étais là, à l'écouter avec des écouteurs. Le père a resserré sa prise sur l'enfant qui s'est redressé et, avec ses sombres yeux en demi-lune, il a regardé directement vers la webcam de l'ordinateur – je n'ai pas pu m'empêcher d'avoir le sentiment que c'est moi qu'il regardait. Je me suis soudain rendu compte que je retenais mon souffle. J'ai fermé la session, je me suis arraché à l'ordi et j'ai quitté le bureau pour gagner les toilettes dans le couloir, la tête baissée, les écouteurs toujours sur les oreilles avec le câble qui pendouillait.
Tout dans cet enfant, tout dans ce père, m'évoquait mon père et moi… »

p. 330.
« *Je pouvais seulement étendre, de manière sans doute idéaliste, la confiance que j'avais en ma famille et en Lindsay à l'ensemble de mes concitoyens, et entretenir l'espoir qu'une fois qu'ils auraient pris la mesure de l'étendue de la surveillance de masse du gouvernement américain, ils se mobiliseraient et ils demanderaient justice.* »

p. 347. (Moscou)
« *Ma présence à l'aéroport est vite devenue un spectacle mondial. Les Russes ont fini par trouver ça pénible. Le 1er juillet le président Bolivien Evo Morales a quitté un autre aéroport à Moscou, Vnoukovo, à bord d'un avion de la flotte gouvernementale après avoir assisté au FPEG, le Forum des pays exportateurs de gaz. Le gouvernement américain, qui soupçonnait ma présence à bord pour la seule raison que le président Morales avait exprimé sa solidarité à mon égard, a fait pression sur les gouvernements italiens, français, espagnol et portugais pour qu'ils refusent à l'avion l'accès à leur espace aérien, est a réussi à le détourner pour l'obliger à atterrir à Vienne, en Autriche. Là-bas, l'avion a été fouillé de fond en comble et n'a été autorisé à redécoller que quand on a été sûr et certain que je n'étais pas planqué quelque part à bord. Il s'agissait d'une violation flagrante de la souveraineté bolivienne, ce que n'a pas manqué de souligner l'ONU.*
L'incident a été un affront pour la Russie, qui n'avait pas pu garantir à un chef d'État en visite de pouvoir rentrer chez lui en toute sécurité. Au passage, l'incident a apporté la confirmation, à la Russie comme à moi,

que n'importe quel vol sur lequel les États-Unis suspecteraient ma présence risquait d'être de la même manière détourné et forcé à atterrir. »

p. 372.
« *Et puis il y a nos données les plus intimes, nos informations génétiques : si nous autorisons qu'elles soient utilisées pour nous identifier, alors elles seront utilisées pour nous persécuter, et même pour nous modifier – pour transformer l'essence même de l'humanité à l'image de la technologie qui cherche à la contrôler*. »