JULIAN ASSANGE,

JACOB APPELBAUM,

ANDY MÜLLER-MAGUHN

ET JÉRÉMIE ZIMMERMANN

MENACE SUR NOS LIBERTÉS

Comment Internet nous espionne

Comment résister

Traduit de l'anglais

par Abel Gerschenfeld et Anatole Muchnik

ROBERT LAFFONT

Titre original : CYPHERPUNKS. FREEDOM AND THE FUTURE OF INTERNET

Traduction française : Éditions Robert Laffont, S.A., Paris, 2013

ISBN 978-2-221-13673-7

(édition originale : ISBN 978-1-939293-00-8, OR Books LLC, New York, édition publiée avec l'accord de OR Books et 2 Seas Literary Agency)

En couverture : © L_amica / Fotolia

© Paul Rogers/The Times/Sipa Press

Introduction

Un cri d'alarme

Ce livre n'est pas un manifeste. Il n'y a plus de temps pour cela. Ce livre est un cri d'alarme.

Le monde n'est pas simplement en train de dériver vers une dystopie transnationale sans précédent – il s'y précipite. Hors des milieux qui s'occupent de la sécurité nationale, cette situation n'a pas été pleinement perçue, occultée par le secret, la complexité et l'ampleur qui la caractérisent. Internet, le meilleur de nos instruments d'émancipation, est devenu le plus redoutable auxiliaire du totalitarisme qu'on n'ait jamais connu. Internet est une menace pour l'humanité.

Si cette transformation n'a pas fait de bruit, c'est parce que ceux qui en sont conscients travaillent dans l'industrie de la surveillance mondiale et n'ont aucun intérêt à prendre la parole. À moins d'un changement de cap, la civilisation mondiale sera devenue d'ici à quelques années une dystopie de surveillance postmoderne, à laquelle seuls les plus habiles auront une chance de se soustraire. En vérité, nous y sommes peut-être déjà.

Une foule d'auteurs ont réfléchi à ce que signifie Internet pour la civilisation mondiale, mais ils se trompent. Ils se trompent parce qu'ils n'ont pas la perspective que procure l'expérience directe. Ils se trompent parce qu'ils n'ont jamais rencontré l'ennemi.

Aucune description du monde ne survit au premier contact avec l'ennemi.

Nous avons rencontré l'ennemi.

Au cours des six dernières années, WikiLeaks s'est heurté à presque toutes les grandes puissances étatiques ou à leurs relais. Parce que nous en avons sondé les secrets, nous avons des nouvelles formes de surveillance étatique une perspective de l'intérieur. Nous en avons une perspective de combattants parce que nous avons été amenés à protéger nos collaborateurs, nos finances et nos informateurs contre ces attaques. Nous en avons une perspective mondiale parce que nous disposons d'alliés, de ressources et d'informations dans quasiment tous les pays. Nous en avons une perspective à long terme, parce que nous luttons contre ce phénomène depuis des années, au cours desquelles nous l'avons vu se démultiplier et se propager sans répit. C'est un parasite invasif, qui se nourrit de toutes les sociétés qui fusionnent avec Internet. Il se répand sur la planète entière, infectant tous les États et les peuples qu'il rencontre.

Que faut-il donc faire ?

Un beau jour, dans un lieu qui ne se trouve nulle part, nous, bâtisseurs et citoyens de l'Internet naissant, avons débattu de l'avenir de notre nouveau monde.

Nous avions compris que les rapports entre peuples seraient désormais médiatisés par notre

nouveau monde et que les États, qui se définissent par la façon dont les gens échangent l'information, les biens et les forces, changeraient de nature eux aussi.

Nous avions compris que la fusion entre les structures étatiques existantes et Internet créait la possibilité d'un changement de nature des États.

Commençons par rappeler que l'État est un système au moyen duquel s'exerce la force de coercition. Les factions au sein d'un État peuvent se disputer l'adhésion des gens, donnant lieu à des phénomènes démocratiques de surface, mais le soubassement d'un État est l'application – et l'évitement – systématique de la violence. La possession de la terre, la propriété, les loyers, les dividendes, les impôts, les amendes judiciaires, la censure, les droits d'auteur et les marques, tout cela est garanti par la menace de l'application de la violence d'État.

Le plus souvent, nous n'avons pas conscience de la proximité de cette violence, parce que nous faisons tous des concessions pour l'éviter. Tel le marin flairant la brise, nous nous attardons peu sur l'idée que notre monde de surface repose sur l'obscurité.

Dans le nouvel espace créé par Internet, quel serait le bras armé de la force coercitive ?

La question a-t-elle seulement un sens ? Dans cet espace éthéré, ce royaume en apparence platonique où circulent les idées et les informations, peut-il vraiment y avoir une force coercitive ? Une force qui modifierait les archives historiques, mettrait les téléphones sur écoute, isolerait les individus, transformerait la complexité en bouillie et érigerait des murs, à la façon d'une armée d'occupation ?

Comme le rappellent ses origines physiques, le flux d'idées et d'informations qu'est Internet n'est pas d'une nature seulement platonique. Internet a pour fondations des câbles de fibre optique posés au fond des océans, des satellites qui tournoient au-dessus de nos têtes, des serveurs informatiques hébergés dans des villes aussi diverses que New York et Nairobi. Tout comme le soldat qui tua Archimède d'un simple coup d'épée, une milice armée pourrait faire main basse sur l'ultime réalisation de la civilisation occidentale, sur notre royaume platonique.

Le nouveau monde d'Internet, se sentant au-dessus du monde physique ordinaire, avait soif d'indépendance. Mais les États et leurs amis sont intervenus pour en prendre le contrôle – en s'assurant la maîtrise de ses fondations matérielles. L'État, comme une armée déployée autour d'un puits de pétrole ou un douanier qui extorque les pots-de-vin à la frontière, a vite appris à profiter de sa maîtrise de l'espace physique pour obtenir celle de notre royaume platonique. Il nous a privés de l'indépendance dont nous avions rêvé puis, en campant sur les lignes de fibre optique et autour des stations satellitaires terrestres, il a entrepris d'intercepter massivement le flux d'informations de notre nouveau monde – son essence même – alors que toutes les relations humaines, économiques et politiques s'y retrouvaient. L'État s'est introduit dans les veines et les artères de nos nouvelles sociétés, engloutissant toute relation exprimée ou communiquée, toute page consultée, tout message émis et toute idée soumise à un moteur de recherche, puis il a stocké ce savoir, des milliards d'interceptions quotidiennes, un pouvoir dont il n'aurait jamais rêvé, dans d'immenses hangars ultrasecrets, à jamais. Il a ensuite entrepris de fouiller et fouiller encore ce trésor, l'expression intellectuelle collective intime de l'humanité, à l'aide d'algorithmes de plus en plus sophistiqués, et de le faire fructifier en poussant au maximum le déséquilibre de pouvoir entre les intercepteurs et le monde des interceptés. L'État a alors rapporté ce qu'il avait appris au monde physique pour déclencher des guerres, guider des drones, manipuler des commissions de l'ONU et négocier des accords, ainsi que pour rendre des services à son vaste réseau interconnecté d'industries, d'initiés et de copains.

Mais nous avons fait une découverte. Celle de notre unique espoir d'échapper à la domination totale. Un espoir qu'avec un peu de courage, de perspicacité et de solidarité nous pourrons utiliser pour résister. Une étrange propriété de l'univers physique dans lequel nous vivons.

L'univers croit au cryptage.

Il est plus facile de crypter l'information que de la décrypter.

Nous avons compris qu'il était possible d'utiliser cette étrange propriété pour créer les lois d'un nouveau monde. Pour libérer notre nouveau royaume platonique de ses fondements constitués de satellites, de câbles sous-marins et de ceux qui les contrôlent. Pour fortifier notre espace derrière un voile cryptographique. Pour créer de nouveaux territoires interdits à ceux qui contrôlent la réalité physique, parce qu'il leur faudrait des ressources infinies pour nous y suivre.

Et pour ainsi déclarer l'indépendance.

Les scientifiques du projet Manhattan ont découvert que l'univers permettait la création de la bombe nucléaire. Cette conclusion n'allait pas de soi. La création d'armes nucléaires aurait pu ne pas être à la portée des lois de la physique. Mais l'univers croit aux bombes atomiques et aux réacteurs nucléaires. Ces phénomènes ont la bénédiction de l'univers, comme le sel, la mer ou les étoiles.

De même, l'univers, notre univers physique, possède cette caractéristique qui permet à un individu, ou à un groupe d'individus, de crypter quelque chose de façon fiable et automatique, sans même en avoir conscience, de sorte que tous les moyens et toute la volonté politique des plus fortes superpuissances du monde ne parviendront pas à le déchiffrer. Et les voies de cryptage entre les individus peuvent fusionner pour créer des régions à l'abri de la force coercitive de l'État extérieur. À l'abri de l'interception massive. À l'abri du contrôle de l'État.

Les gens peuvent ainsi opposer leur libre arbitre à celui d'une superpuissance mobilisant tous ses moyens, et l'emporter. Le cryptage est une incarnation des lois de la physique, il est indifférent aux fanfaronnades des États, et même aux dystopies de surveillance transnationale.

Le monde aurait pu fonctionner d'une autre manière. Mais, allez savoir pourquoi, l'univers voit le cryptage d'un bon œil.

La cryptographie est la forme la plus aboutie de l'action directe non violente.

Les États qui possèdent l'arme nucléaire ont beau pouvoir exercer une violence sans limites sur des millions d'individus, l'existence d'une cryptographie puissante signifie qu'un État ne peut rien contre la volonté d'individus de garder des secrets, même en exerçant une violence sans bornes.

Une cryptographie puissante permet de résister à l'application illimitée de la violence. Aucune force de coercition ne parviendra jamais à résoudre un problème mathématique.

Est-il possible pour autant de tirer avantage de cet étrange état de choses pour construire une composante émancipatrice fondamentale de l'indépendance de l'humanité dans ce royaume platonique qu'est Internet ? Et lorsque les sociétés fusionnent avec Internet, peut-on appliquer à son tour cette liberté à la réalité physique pour redéfinir l'État ?

Rappelons que l'État est le système qui détermine où et comment la coercition est systématiquement appliquée.

La réponse à la question de savoir quelle quantité de force coercitive est susceptible de filtrer du monde physique vers le royaume platonique d'Internet est donnée par la cryptographie et les idéaux des cypherpunks1.

Dans la mesure où l'État fusionne avec Internet, l'avenir de notre civilisation devient l'avenir d'Internet, et il faut redéfinir le rapport de force.

Si nous ne le faisons pas, l'universalité d'Internet transformera l'humanité en un vaste réseau de surveillance et de contrôle des masses.

Il faut donner l'alerte. Ce livre est le cri d'une sentinelle dans la nuit.

Le 20 mars 2012, alors que j'étais assigné à résidence au Royaume-Uni en attendant mon extradition, j'ai rencontré trois amis, sentinelles comme moi, avec l'idée que nos voix mises à l'unisson réveilleraient peut-être la cité. Nous devons communiquer ce que nous avons appris tant que nous le pouvons.

Notre tâche est d'assurer l'autodétermination partout où cela est possible, de contenir la dystopie annoncée là où cela ne l'est pas ou, en dernier recours, de précipiter son autodestruction.

Julian Assange, Londres, octobre 2012

1. Les cypherpunks (de l'anglais cipher – chiffrement – et punk) militent pour le recours à la cryptographie (du grec kryptos – écriture secrète –, pratique consistant à communiquer en langage codé) et à des méthodes du même type comme instrument de changement social et politique. Fondé au début des années 1990, leur mouvement a été particulièrement actif lors des « guerres du cryptage » qui ont secoué la décennie, puis après le printemps Internet de 2011. Le terme a fait son entrée dans l'Oxford English Dictionary en 2006 (« Oxford English Dictionary Updates Some Entries & Adds New Words ; Bada-Bing, Cypherpunk, and Wi-Fi Now in the OED », ResourceShelf, 16 septembre 2006 : http://web.resourceshelf.com/go/resourceblog/43743 [lien vérifié le 22 novembre 2012])

Les participants à la discussion

Julian ASSANGE est le rédacteur en chef et l'esprit visionnaire de WikiLeaks1. Contributeur de la première heure à la liste de diffusion Cypherpunk, Julian est aujourd'hui l'un des porte-parole les plus actifs de la philosophie cypherpunk. Son travail avec WikiLeaks a donné une réalité politique à la formule cypherpunk : « Vie privée pour les faibles, transparence pour les puissants. » Rendu célèbre par l'exercice vigoureux de la liberté d'expression en vue d'imposer la transparence et la responsabilité aux puissants, Julian est aussi un critique virulent de l'intrusion des États et des

entreprises dans la vie privée des individus. Il est à l'origine de nombreux projets s'inscrivant dans la ligne de la philosophie cypherpunk, comme strobe.c, le premier scanner de port TCP/IP, le système de chiffrement niable de documents Rubberhose2 et le premier code source de WikiLeaks. Alors qu'il était adolescent, Julian a fait partie des premiers spécialistes en sécurité informatique et de réseaux, avant que certaines formes de hacking soient considérées comme des activités criminelles. Julian a ensuite été activiste et fournisseur d'accès Internet en Australie pendant les années 1990. Il est également le coauteur avec Suelette Dreyfus de Underground, une histoire du mouvement international des hackers dont s'est librement inspiré le film Underground: The Julian Assange Story3.

Jacob APPELBAUM est l'un des fondateurs de Noisebridge4, à San Francisco, il est membre du Chaos Computer Club de Berlin. C'est également un développeur. C'est aussi l'un des personnages clés du Tor Project5, un système d'anonymat en ligne permettant à chacun de résister à la surveillance et à la censure sur Internet. Depuis dix ans il apporte son aide aux militants écologistes et des droits de l'homme, travail qui l'a conduit à publier des recherches innovantes sur la sécurité, le droit à la vie privée et l'anonymat dans un certain nombre de domaines, allant de la médecine légale informatisée au cannabis médical. Jacob estime que chacun a le droit de lire, sans restriction, et de parler librement, sans exception. En 2010, lorsque Julian Assange s'est trouvé dans l'impossibilité de donner une conférence à New York, c'est Jacob qui a pris sa place. Depuis, tout comme ses amis et sa famille, il subit le harcèlement des autorités des États-Unis : interrogatoires dans les aéroports, fouilles au corps très poussées accompagnées de menaces à peine voilées de sévices à venir en prison ; son matériel a été confisqué et les sites qu'il utilisait pour ses services en ligne ont reçu ordonnance d'injonction de remettre toutes les informations le concernant, avec interdiction de l'avertir. Refusant de se laisser intimider, Jacob continue de se défendre dans les procédures en cours contre lui et de prendre ouvertement la défense de la liberté d'expression, tout en soutenant activement WikiLeaks.

Andy MÜLLER-MAGUHN est membre de longue date du Chaos Computer Club allemand, dont il a été l'un des dirigeants ainsi que le porte-parole6. C'est l'un des fondateurs d'EDRI7, European Digital Rights, une ONG qui se bat pour le respect des droits de l'homme à l'ère numérique. De 2000 à 2003, il a été élu par les usagers européens d'Internet directeur européen de l'ICANN8, l'Internet Corporation for Assigned Names and Numbers (société pour l'attribution des noms de domaine et des numéros sur Internet), qui décide à l'échelon planétaire de la façon dont doivent s'organiser les « noms et les nombres » d'Internet. C'est un spécialiste de la surveillance dans le domaine des télécommunications et, à ce titre, il travaille en tant que journaliste sur l'industrie de la surveillance dans le cadre de son projet wiki, buggedplanet.info9. Andy s'occupe également de cryptographie et a créé avec d'autres une entreprise nommée Cryptophone10, qui commercialise des dispositifs de sécurisation des communications vocales et exerce une activité de conseil stratégique dans le contexte de l'architecture de réseaux.

Jérémie ZIMMERMANN est le cofondateur et le porte-parole de La Quadrature du Net11, première organisation européenne de défense du droit des citoyens à l'anonymat sur Internet, réputée pour sa dénonciation des tentatives de régulation de la liberté en ligne. Jérémie participe à l'élaboration d'outils participatifs permettant au plus grand nombre de faire changer les choses. Il est très impliqué dans les débats sur le droit d'auteur, la neutralité du Net et d'autres sujets décisifs pour l'avenir d'un Internet libre. La Quadrature du Net a récemment obtenu une victoire historique en

menant une campagne qui a fait échouer l'Anti-Counterfeiting Trade Agreement (ACTA, Accord commercial anticontrefaçon) au Parlement européen. Peu après avoir pris part à la discussion qui constitue ce livre, Jérémie a été interpellé par deux agents du FBI au moment de quitter les États-Unis, et subi un interrogatoire à propos de WikiLeaks.

1. WikiLeaks : http://wikileaks.org

2. Pour en savoir plus sur le dossier Rubberhose, voir « The Idiot Savants' Guide to Rubberhose », de Suelette Dreyfus : http://marutukku.org/current/src/doc/maruguide/t1.html (lien vérifié le 22 novembre 2012).

3. Pour en savoir plus sur le film Underground, voir : http://www.underground-book.net. Pour en savoir plus sur le film Underground: The Julian Assange Story, voir l'Internet Movie Database : http://www.imdb.com/title/tt2357453/ (liens vérifiés le 22 novembre 2012).

4. Noisebridge, établi à San Francisco, est un hackerspace, c'est-à-dire un fournisseur d'infrastructures pour des projets techniques créatifs. Il est collectivement géré par ses membres : https://www.noisebridge.net/wiki/Noisebridge. Le Chaos Computer Club Berlin est l'antenne berlinoise du Chaos Computer Club : https://berlin.ccc.de/wiki/Chaos_Computer_Club_Berlin. (liens vérifiés le 22 novembre 2012).

5. Tor Project : https://www.torproject.org

6. Le Chaos Computer Club est la plus grande organisation européenne de hackers. Ses activités vont de la recherche et l'exploration techniques à la tenue de campagnes, d'événements, de publications et de conseil stratégique : http://www.ccc.de

7. EDRI : http://www.edri.org

8. ICANN : http://www.icann.org

9. buggedplanet : http://buggedplanet.info

10. Cryptophone : http://www.cryptophone.de

11. La Quadrature du Net : http://www.laquadrature.net

Note de l’éditeur

Pour rendre Menace sur nos libertés plus accessible au lecteur ordinaire, chacun des participants à la discussion a eu la possibilité de développer, clarifier ou annoter ses arguments autant qu’il le voulait. La mise en ordre générale du manuscrit respecte la dynamique de la discussion d’origine.

À propos des diverses tentatives

de persécution de WikiLeaks

et des individus qui y sont associés

La discussion qui suit contient de nombreuses références à des événements récents dans l’histoire de WikiLeaks. Ces faits étant peut-être inconnus de certains lecteurs, nous avons choisi de les exposer en préambule.

WikiLeaks a pour mission de recueillir des informations fournies par des donneurs d’alerte, de les livrer au public puis de se défendre contre les inévitables attaques légales et politiques. Il est devenu habituel pour les grandes puissances et les grandes organisations de tenter de supprimer les publications de WikiLeaks qui, en tant qu’éditeur de dernier recours, a été conçu pour résister à cette pression.

En 2010, WikiLeaks a lancé sa série de publications la plus réputée à ce jour, qui révélait le recours abusif et systématique au secret officiel par l’armée et le gouvernement des États-Unis. Ces publications sont connues sous les noms de Collateral Murder, War Logs et Cablegate1. En réaction, le gouvernement des États-Unis et ses alliés ont entrepris une action concertée, toujours en cours, visant à détruire WikiLeaks.

Le jury d’accusation contre WikiLeaks

En réaction directe aux publications de WikiLeaks, le gouvernement des États-Unis a ouvert une enquête criminelle sur Julian Assange ainsi que sur le personnel, les sympathisants et les partenaires supposés de WikiLeaks. Un jury d’accusation (grand jury) a été constitué à Alexandria, en Virginie, à l’instigation du département de la Justice et du FBI, pour étudier les poursuites éventuelles contre Julian Assange et d’autres, notamment pour conspiration au titre de l’Espionage Act de 1917. Les représentants de l’État américain ont eux-mêmes déclaré qu’il s’agit d’une enquête « sans précédent par son échelle et sa nature ». La procédure du jury d’accusation se déroule sans la présence d’un juge ou d’un avocat de la défense. Depuis, plusieurs membres du Congrès ont suggéré lors d’auditions devant des commissions du Congrès des États-Unis que l’Espionage Act pouvait servir à cibler des journalistes qui « publient délibérément des informations provenant de fuites », ce qui laisse à penser que cet angle d’attaque est en voie de banalisation pour la justice américaine2.

À la date de parution de ce livre, l'enquête sur WikiLeaks se poursuit3. Plusieurs individus ont été contraints par voie légale de livrer des éléments. Les minutes du procès de Bradley Manning, le soldat accusé d'avoir transmis des informations à WikiLeaks, révèlent l'existence d'un dossier du FBI sur l'enquête WikiLeaks qui fait plus 42 100 pages, dont environ 8 000 sont consacrées à Bradley Manning. Celui-ci a passé plus de 880 jours en prison sans avoir été jugé. Le rapporteur spécial des Nations unies sur la torture, Juan Méndez, a officiellement constaté que Bradley Manning avait subi des traitements cruels et inhumains susceptibles de constituer des actes de torture4.

Appels au meurtre de Julian Assange et groupes de travail visant officiellement WikiLeaks

L'enquête du jury d'accusation n'est pas le seul angle de l'attaque portée contre WikiLeaks. En décembre 2010, dans le sillage du Cablegate, plusieurs responsables politiques américains ont réclamé l'assassinat extrajudiciaire de Julian Assange, si nécessaire par l'intermédiaire d'un drone. Des sénateurs américains ont qualifié WikiLeaks d'« organisation terroriste » et Assange de « terroriste high-tech » et de « combattant ennemi » participant à la « cyberguerre »5.

Au Pentagone, une équipe de 120 personnes a été constituée sous le nom de WikiLeaks Task Force, ou WTF, après la publication des Iraq War Logs et du Cablegate, pour envisager les « actions à mener » contre WikiLeaks. D'autres groupes de travail officiels ont aussi été constitués au FBI, à la CIA et au Département d'État américain6.

Censure directe

Commettant un acte de censure sans précédent à l'égard d'une publication journalistique, l'État américain a fait pression sur des fournisseurs d'accès Internet pour qu'ils interrompent le service de WikiLeaks.org. Le 1er décembre 2010, Amazon a retiré WikiLeaks de ses serveurs d'hébergement et, le 2 décembre, le prestataire DNS a mis fin au nom de domaine WikiLeaks.org. WikiLeaks n'est alors resté en ligne que grâce à un effort collectif de « miroir de masse » qui a vu des milliers de sympathisants de WikiLeaks copier les données du site pour en héberger leur propre version, distribuant les adresses IP à travers les réseaux sociaux7.

L'administration Obama a averti les employés fédéraux que les documents rendus publics par WikiLeaks demeuraient confidentiels – bien qu'ils aient été publiés dans les pages de certains des principaux organes de presse du monde, dont le New York Times ou le Guardian. Les employés ont été avertis que toute consultation de ces documents, que ce soit sur WikiLeaks.org ou dans le New York Times, serait considérée comme une infraction à la sécurité8. Les organismes d'État comme la bibliothèque du Congrès, le département du Commerce ou l'armée américaine ont bloqué sur leurs réseaux l'accès aux documents WikiLeaks. L'interdiction ne s'est pas cantonnée au secteur public. Des employés de l'État américain ont averti les institutions universitaires que les étudiants se destinant à une carrière dans l'administration devraient se tenir à l'écart des documents rendus publics par WikiLeaks lors de leurs travaux de recherche et dans leurs activités en ligne.

Censure financière : le blocus bancaire

WikiLeaks est financé par les dons de ses sympathisants. En décembre 2010, cédant aux pressions officieuses américaines, certaines institutions financières et bancaires importantes, dont Visa, MasterCard, PayPal et Bank of America, ont refusé leurs services financiers à WikiLeaks. Elles ont bloqué les virements bancaires et toute donation effectuée par le biais des principales cartes de crédit. Ce sont des institutions américaines, mais leur omniprésence dans le monde de la finance a eu pour conséquence que des donateurs américains ou du reste du monde se sont vu refuser la

possibilité d'envoyer de l'argent à WikiLeaks pour soutenir ses activités.

Ce « blocus bancaire », comme on l'a appelé, a été mis en place en dehors de toute procédure judiciaire ou administrative et reste en vigueur au moment où paraît ce livre. WikiLeaks a engagé d'importantes poursuites judiciaires dans différentes juridictions du monde pour y mettre fin, obtenant certaines victoires préliminaires, et les procédures suivent leur cours. Entre-temps, WikiLeaks a été privé de revenus, a dû faire face à des frais élevés et opère depuis près de deux ans sur des fonds de réserve.

Le blocus bancaire est l'affirmation par le pouvoir lui-même qu'il contrôle les transactions financières entre tiers. C'est une atteinte directe à la liberté économique des individus. Au-delà de ce point précis, la menace existentielle qu'il fait peser sur WikiLeaks illustre une nouvelle forme troublante de censure économique mondiale9.

Certaines personnes censées être liées à WikiLeaks, ainsi que des sympathisants et des membres du personnel, ont connu de mystérieux ennuis avec leur compte bancaire – allant d'incidents concernant l'activité du compte à sa clôture pure et simple.

Harcèlement de Jacob Appelbaum

et de Jérémie Zimmermann

Le 17 juillet 2010, Julian Assange était censé prendre la parole à la conférence de hackers HOPE, à New York. Il a dû annuler son intervention, et c'est Jacob Appelbaum qui l'a remplacé. Depuis ce jour, les forces de l'ordre mènent une campagne de harcèlement contre Appelbaum et son entourage. Celui-ci est arrêté, fouillé et interrogé en l'absence de tout avocat dès qu'il entre ou sort des États-Unis. Son matériel a été saisi et ses droits violés, et il a été menacé de violations supplémentaires de ses droits. Les gardes à vue et le harcèlement qu'il a subis sont le fait de divers services américains, dont le département de Sécurité intérieure (Homeland Security), les services de l'immigration et des douanes et l'armée des États-Unis. Lors de ces gardes à vue, pour accentuer la pression, il lui a même été interdit de se rendre aux toilettes. À aucun moment Appelbaum n'a été formellement accusé ni informé par les autorités des motifs de ce harcèlement10.

À la mi-juin 2011, alors qu'il s'apprêtait à embarquer dans un avion à l'aéroport Dulles de Washington, Jérémie Zimmermann a été interpellé par deux hommes qui se sont identifiés comme des agents du FBI. Ceux-ci l'ont interrogé à propos de WikiLeaks en le menaçant de l'arrêter et de le mettre en prison.

Appelbaum et Zimmermann font partie de la longue liste d'amis, de sympathisants ou d'associés supposés de Julian Assange qui ont été victimes du harcèlement et de la surveillance des services américains, une liste sur laquelle figurent des avocats et des journalistes dans l'exercice de leur profession.

Saisie sans mandat d'archives électroniques

et « affaire de l'injonction de Twitter »

Le 14 décembre 2010, Twitter a reçu une « injonction administrative » du département américain de la Justice lui intimant de remettre toute information relative à une enquête sur WikiLeaks. Cette injonction était prétendument un « ordre 2703(d) », en référence à un article du Stored Communications Act, la loi sur le stockage de communications électroniques. Par cette loi, l'État américain s'octroie l'autorité d'exiger la divulgation des archives de communications électroniques

privées sans intervention d'un juge – ce qui lui permet de contourner le dispositif de protection prévu par le IVe amendement contre la fouille et la saisie arbitraires.

L'injonction visait à obtenir des noms d'utilisateur des archives de correspondance, des adresses, des numéros de téléphone, des relevés d'identité bancaires et des numéros de carte de crédit correspondants à des comptes et des individus prétendument liés à WikiLeaks, parmi lesquels Jacob Appelbaum, la parlementaire islandaise Birgitta Jónsdóttir, l'homme d'affaires hollandais et pionnier d'Internet Rop Gonggrijp, travaillant pour WikiLeaks. Selon les termes de l'injonction, Twitter n'avait même pas le droit d'informer les personnes visées de l'existence de cette injonction. Twitter a contesté cette clause avec succès et obtenu le droit d'informer les intéressés que leurs archives étaient réquisitionnées.

Après avoir été avisés par Twitter de cette injonction, Appelbaum, Jóndósttir et Gonggrijp, représentés par Keker & Van Nest, l'American Civil Liberties Union et l'Electronic Frontier Foundation, ont demandé à leurs avocats de porter collectivement plainte pour faire annuler cet ordre. Cette plainte a reçu le nom d'« affaire de l'injonction de Twitter11 ». Une autre requête a été déposée par l'avocat d'Appelbaum réclamant la divulgation des archives judiciaires secrètes concernant les tentatives par l'État de mettre la main sur ses données privées chez Twitter et d'autres entreprises. Les deux requêtes ont été refusées par un juge le 11 mars 2011. Les plaignants ont fait appel.

Le 9 octobre 2011, le Wall Street Journal a révélé que le service californien de messagerie Sonic.net avait également reçu une injonction réclamant les données de Jacob Appelbaum. Sonic avait contesté l'injonction de l'État et perdu, mais obtenu l'autorisation d'informer Appelbaum qu'il avait été contraint de céder les informations le concernant. Le Wall Street Journal faisait état d'une injonction du même type adressée à Google, sans préciser si ce dernier l'avait contestée devant la justice12.

Le 10 novembre 2011, un juge fédéral a statué contre Appelbaum, Jónsdóttir et Gonggrijp, et ordonné à Twitter de remettre ses informations au département de la Justice13. Le 20 janvier 2012, les plaignants ont de nouveau fait appel pour contester le refus de lever le secret sur les injonctions envoyées à d'autres entreprises que Twitter14. Au moment où paraît ce livre, l'appel est toujours en cours.

1. Collateral Murder : http://www.collateralmurder.com

The Iraq War Logs : http://wikileaks.org/irq

The Afghan War Diary : http://wikileaks.org/afg

Cablegate : http://wikileaks.org/cablegate.html

2. « Congressional committee holds hearing on national security leak prevention and punishment », Reporters Committee for Freedom of the Press, 11 juillet 2012 : http://www.rcfp.org/browse-media-law-resources/news/congressional-committee-holds-hearing-national-security-leak-prevent (lien vérifié le 24 novembre 2012).

3. Pour plus d'informations sur le jury d'accusation saisi du cas WikiLeaks, voir la chronologie établie par la journaliste indépendante Alexa O'Brien : http://www.alexaobrien.com/timeline_us_versus_manning_assange_wikileaks_2012.html (lien vérifié le 24 novembre 2012).

4. « Bradley Manning's treatment was cruel and inhuman, UN torture chief rules », The Guardian, 12 mars 2012 : http://www.guardian.co.uk/world/2012/mar/12/bradley-manning-cruel-inhuman-treatment-un (lien vérifié le 24 novembre 2012).

5. « WikiLeaks: guilty parties "should face death penalty" », The Telegraph, 1er décembre 2010 : http://www.telegraph.co.uk/news/worldnews/wikileaks/8172916/WikiLeaks-guilty-parties-should-face-death-penalty.html (lien vérifié le 24 novembre 2012).

6. « CIA launches task force to assess impact of U.S. cables' exposure by WikiLeaks », Washington Post, 22 décembre 2010 : http://www.washingtonpost.com/wp-dyn/content/article/2010/12/21/AR2010122104599.html?hpid=topnews&sid=ST2010122105304 (lien vérifié le 24 novembre 2012).

7. « WikiLeaks fights to stay online after US company withdraws domain name », The Guardian, 3 décembre 2012 : http://www.guardian.co.uk/media/blog/2010/dec/03/ wikileaks-knocked-off-net-dns-everydns?INTCMP=SRCH (lien vérifié le 24 novembre 2012).

8. « Don't Look, Don't Read: Government Warns Its Workers Away From WikiLeaks Documents », New York Times, 4 décembre 2010 : http://www.nytimes.com/2010/ 12/05/world/05restrict.html?hp&_r=2& (lien vérifié le 24 novembre 2012).

9. « Banking Blockade », WikiLeaks : http://www.wikileaks.org/Banking-Blockade.html (lien vérifié le 24 novembre 2012).

10. Le récit écrit par Jacob des arrestations qu'il a subies mérite d'être lu. Voir : « Air Space – a trip through an airport detention center », Boing Boing, 31 octobre 2011 :

http://boingboing.net/2011/10/31/air-space-a-trip-through-an-ai.html. Lire aussi une interview de Jacob dans Democracy Now sur les arrestations survenues. « National Security Agency Whistleblower William Binney on Growing State Surveillance », Democracy Now, 20 avril 2012 : http://www.democracynow.org/2012/4/20/exclusive_national_security_agency_whistleblower_william (liens vérifiés le 24 novembre 2012).

11. L'intitulé officiel de l'affaire est : In the Matter of the 2703(d) Order Relating to Twitter Accounts: WikiLeaks Rop_G IOERROR ; and BirgittaJ.

12. « Secret orders target email », Wall Street Journal, 9 octobre 2011 : http://online.wsj.com/article/SB10001424052970203476804576613284007315072.html (lien vérifié le 24 novembre 2012).

13. « Twitter Ordered to Yield Data in WikiLeaks Case », New York Times, 10 novembre 2011 : https://www.nytimes.com/2011/11/11/technology/twitter-ordered-to-yield-data-in-wikileaks-case.html?_r=1 (lien vérifié le 24 novembre 2012).

14. « ACLU & EFF to Appeal Secrecy Ruling in Twitter/WikiLeaks Case », communiqué de presse de l'Electronic Frontier Foundation, 20 janvier 2012 : https://www.eff.org/press/releases/aclu-eff-appeal-secrecy-ruling-twitterwikileaks-case (lien vérifié le 24 novembre 2012).

Plus de communication

ou plus de surveillance ?

JULIAN : Si on remonte au début des années 1990, quand le mouvement cypherpunk a pris de l'ampleur en réaction à l'interdiction de la cryptographie par les États, beaucoup ont pensé qu'Internet, par sa puissance, permettrait des communications libres de toute censure, par opposition aux grands médias. Mais les cypherpunks savaient depuis le début que, de fait, ce pouvoir s'accompagnerait de celui de surveiller toutes les communications qui se produisaient. Aujourd'hui, la question est : plus de communication ou plus de surveillance ? Plus de communication veut dire plus de liberté vis-à-vis des gens qui cherchent à contrôler les idées et à fabriquer du consensus, plus de surveillance veut dire précisément l'inverse.

La surveillance est nettement plus perceptible aujourd'hui qu'à l'époque où elle était l'apanage des Américains, des Britanniques, des Russes et de quelques autres États, comme la Suisse et la France. Elle est aujourd'hui pratiquée par tout le monde, et par à peu près tous les États, à cause de la commercialisation des techniques de surveillance de masse. Et elle est en train de devenir totale, parce que tout le monde met sur Internet ses opinions politiques, ses échanges familiaux et amicaux. On n'assiste donc pas simplement à une surveillance accrue des communications qui existaient, mais à une explosion des communications à surveiller. Des communications qui ont augmenté en

volume mais aussi en variété, en devenant de plus en plus intimes. Toutes ces nouvelles communications, hier circonscrites à la sphère privée, sont aujourd'hui massivement interceptées.

Une bataille est en cours entre d'une part la puissance que confèrent ces informations recueillies par des initiés, ces États fantômes de l'information qui sont en train de se développer, interchangeables, multipliant les liens entre eux et avec le secteur privé, et d'autre part la prolifération d'espaces partagés où Internet est un outil qui permet aux hommes de se parler.

Je voudrais réfléchir à la façon dont nous présentons nos idées. Le grand problème que je rencontre, en tant qu'individu baignant dans la surveillance étatique et qui sait à quel point l'industrie de la sécurité transnationale s'est développée depuis vingt ans, c'est que tout cela m'est trop familier, et cela m'empêche de voir le problème du point de vue du citoyen ordinaire. Or, le monde que nous connaissons tous les quatre est à présent devenu celui de tous, parce que chacun a confié le cœur même de son existence à Internet. Il faut d'une façon ou d'une autre que nous communiquions ce que nous savons tant que cela reste possible.

ANDY : Je suggère de ne pas adopter le point de vue du citoyen, mais celui des individus au pouvoir. L'autre jour, je me suis retrouvé dans une drôle de conférence à Washington où il y avait des types qui portaient le badge de l'ambassade d'Allemagne. Je leur ai dit : « Ah, vous êtes de l'ambassade d'Allemagne », et ils m'ont répondu : « Euh, pas exactement, en fait on vient du côté de Munich. » J'ai appris que c'était des agents du renseignement extérieur et, pendant le dîner, je leur ai demandé : « Alors, à quoi sert le secret ? » Ils m'ont répondu : « Ça permet de ralentir les processus afin de mieux les contrôler. » C'est le cœur même de ce type de travail de renseignement que de ralentir l'évolution d'un processus en privant les gens de la possibilité de le comprendre. En déclarant qu'une chose est secrète, on réduit le nombre d'individus qui comprennent et sont donc capables d'influencer le processus.

Quand on regarde Internet du point de vue des gens au pouvoir, les vingt dernières années ont été terrifiantes. Ils ont vu débarquer Internet comme une maladie qui les prive de leur capacité à définir le réel, à définir le cours des choses, ce qui sert ensuite à définir ce que les gens savent du cours des choses et leurs propres aptitudes à y intervenir. Prenons l'Arabie saoudite, par exemple, où un hasard historique a voulu que les chefs religieux possèdent aussi l'essentiel du pays ; leur intérêt au changement est proche de zéro. Quelque part entre zéro et moins cinq peut-être. Internet leur apparaît comme une maladie, alors ils demandent à leurs conseillers : « Avez-vous un remède contre ce truc qui se propage ? Il faut nous immuniser au cas où ça affecterait notre pays, au cas où cet Internet machinchouette viendrait chez nous. » Et la réponse, c'est la surveillance de masse. C'est : « Il faut avoir le contrôle de tout, il faut tout filtrer, il faut qu'on sache tout ce qu'ils font. » C'est ça qui s'est produit depuis vingt ans. Les individus au pouvoir ont énormément investi dans la surveillance parce qu'ils ont eu peur qu'Internet menace leur mode de gouvernement.

JULIAN : Pourtant, malgré cette surveillance de masse, les communications de masse ont permis à des millions d'individus de parvenir rapidement à un consensus. S'il est possible de passer très vite d'une position normale à une nouvelle position de consensus de masse, l'État aura beau le voir se développer, il n'aura pas le temps de formuler une réaction efficace.

Cela dit, en 2008, il y a eu au Caire une manifestation organisée à partir de Facebook. Elle a surpris le gouvernement Moubarak, et ces gens ont fini par être traqués à travers Facebook1. En 2011, dans un manuel qui est devenu l'un des principaux do- cuments ayant servi à la révolution égyptienne, on

peut lire dès les premières pages « N'utilisez pas Twitter ou Facebook » pour distribuer ce manuel2. Beaucoup d'Égyptiens ont utilisé Twitter et Facebook malgré tout. Ils n'ont survécu que parce que la révolution a réussi. Si ça n'avait pas été le cas, ces gens seraient aujourd'hui dans une situation très, très difficile. Et n'oublions pas que le président Moubarak a coupé Internet en Égypte assez tôt. On peut légitimement se demander si cette interruption d'Internet a servi la révolution ou si elle lui a fait du tort. Certains estiment qu'elle l'a aidée, parce qu'elle a obligé les gens à descendre dans la rue pour savoir ce qui se passait et, une fois qu'on est dans la rue, on est dans la rue. Et les gens ont été directement affectés parce que leur téléphone et leur connexion à Internet ne fonctionnaient plus.

Alors, pour que ça réussisse, il faut une masse critique, il faut que ça se fasse rapidement et il faut que ça gagne, sinon l'infrastructure même, qui permet le développement d'un consensus rapide, servira à traquer et à marginaliser ceux qui se sont impliqués dans la recherche de ce consensus.

Ça, c'était en Égypte, un pays qui était certes l'allié des États-Unis, mais ne fait pas partie de l'alliance anglophone du renseignement constituée par les États-Unis, le Royaume-Uni, l'Australie, la Nouvelle-Zélande et le Canada. Essayons à présent d'imaginer ce qui se serait passé si la révolution égyptienne avait commencé aux États-Unis – que seraient devenus Facebook et Twitter ? Ils auraient été confisqués par l'État. Et si la révolution n'avait pas abouti, ils auraient été fouillés, comme ils le sont en ce moment, par la CIA et le FBI pour obtenir des détails sur l'identité des principaux participants.

JÉRÉMIE : On peut difficilement dissocier surveillance et contrôle. Il faut tenir compte des deux. C'est surtout ça qui m'intéresse – le contrôle d'Internet, que ce soit par des gouvernements ou par des entreprises.

JACOB : Je pense qu'il est assez clair que la censure est un sous-produit de la surveillance au sens général, aussi bien l'autocensure que la censure technique, et il me semble qu'il est important de l'expliquer aux gens en des termes non techniques. Par exemple, si on construisait les routes comme on construit Internet, chacune serait dotée de caméras et de micros de surveillance auxquels nul n'aurait accès sauf la police, ou quelqu'un qui réussirait à se faire passer pour la police.

JULIAN : Jacob, c'est ce qui est en train de se produire au Royaume-Uni.

JACOB : Quand on construit une route, personne n'exige que chaque centimètre puisse être surveillé par un groupe secret d'individus et seulement ce groupe. On peut expliquer à l'homme de la rue que c'est comme ça qu'on est en train de construire les routes d'Internet qu'on lui demandera d'emprunter – c'est une image parlante qui permettra aux gens de comprendre que le détenteur du contrôle de la route ne sera pas éternellement le constructeur d'origine.

ANDY : Mais il y en a qui ne construisent même pas de routes. Ils créent un jardin, là, et invitent tout le monde à s'y balader à poil. C'est ça, Facebook ! C'est un business plan qui vise à faire avaler aux gens l'idée de révéler leurs données.

JACOB : Tout juste. En RDA, les gens étaient payés s'ils collaboraient avec la Stasi – les services de sécurité – et, aujourd'hui, ceux qui vont sur Facebook reçoivent aussi une gratification. La seule différence, c'est qu'avec Facebook il s'agit d'une gratification sociale – ils pourront coucher avec le voisin au lieu de recevoir de l'argent. Et il est important d'en souligner l'aspect humain, parce que ce n'est pas une affaire de technologie, c'est une affaire de surveillance de la pensée. C'est le panoptique idéal, d'une certaine façon3.

JULIAN : Je trouve quand même que la philosophie de la technique est plutôt intéressante. La technique, ce n'est pas seulement un bout de technologie, c'est, par exemple, le consensus majoritaire d'un conseil d'administration, ou la structure d'un Parlement – la systématisation de ses interactions. Par exemple, je pense que le système féodal découle de la technique du moulin. À partir du moment où il y avait des moulins centralisés, requérant d'immenses investissements et faciles à contrôler physiquement, il était assez naturel de se retrouver à l'arrivée avec des rapports féodaux. Avec le temps, nous avons manifestement développé des techniques de plus en plus sophistiquées. Certaines peuvent être démocratisées ; on peut les étendre à tout le monde. Mais, pour la plupart – à cause de leur complexité –, ces techniques prennent forme en tant que fruit d'organisations fortement interconnectées, comme Intel. Peut-être est-il inhérent à la technique de traverser ces phases successives de découverte, de centralisation puis de démocratisation – une fois que la recette de fabrication est transmise à la génération suivante, qui est donc instruite. Mais je crois que, de façon générale, la technique a tendance à centraliser le contrôle entre les mains de ceux qui maîtrisent les ressources physiques nécessaires.

La fabrication de semi-conducteurs en est, à mon sens, le meilleur exemple, quand on voit le degré de maîtrise technique que cela suppose. Dans ces usines, l'air doit être pur, et donc des milliers d'individus doivent porter des filets sur la tête pour éviter que la moindre petite pellicule de peau, le moindre poil ne vienne troubler la fabrication de ces semi-conducteurs, selon un processus à multiples étapes extrêmement complexe. La mise en place de ce processus a demandé, littéralement, des millions d'heures de recherche. Et si ces choses sont populaires, et elles le sont, et si elles sous-tendent Internet, alors la fabrication de semi-conducteurs est inscrite au cœur de la libération d'Internet. Et au cœur de la fabrication de semi-conducteurs s'inscrit la capacité, pour celui qui détient le contrôle physique de cette fabrication, d'arracher d'immenses concessions.

Si bien que ce qui sous-tend la révolution high-tech des communications – et la liberté qui en a découlé –, c'est l'ensemble de l'économie de marché moderne néolibérale, transnationale et mondialisée. L'une est en fait la pointe de l'autre. C'est le maximum, en termes de réalisation technologique, que puisse produire l'économie moderne mondialisée néolibérale. Internet est sous-tendu par le jeu d'interactions commerciales extrêmement complexe entre les fabricants de fibre optique, de semi-conducteurs, les compagnies minières qui extraient tous ces matériaux, et l'ensemble des lubrifiants financiers qui rendent les transactions possibles, les tribunaux pour assurer le respect des lois de la propriété privée et ainsi de suite. Il s'agit donc bien du sommet de la pyramide du système néolibéral tout entier.

ANDY : Concernant l'argument sur la technique, quand Johannes Gutenberg a inventé l'imprimerie, celle-ci a été ponctuellement interdite dans certaines régions d'Allemagne, et c'est précisément ce qui lui a permis de se répandre dans tout le pays, parce que lorsqu'elle était interdite

dans une région, elle se déplaçait vers une autre juridiction4. Je n'ai pas étudié tout ça dans le détail, mais ce que je sais, c'est que l'Église catholique était contre parce que ça cassait le monopole sur la fabrication de livres, et que, chaque fois qu'il y avait des ennuis juridiques, on se déplaçait là où ce n'était pas interdit. D'une certaine façon, cela a contribué à sa propagation.

L'Internet, à mon sens, c'est un peu différent parce qu'on a d'un côté des machines qui peuvent servir en tant que matériel de production – dont le Commodore 64, d'une certaine façon, même si la plupart des gens l'utilisaient à autre chose.

JULIAN : Sur chaque petite machine, on pouvait faire tourner son propre logiciel.

ANDY : Oui. Et on pouvait aussi s'en servir pour diffuser des idées. Mais d'un autre côté, sur le plan philosophique, comme l'a dit John Gilmore – l'un des fondateurs de l'Electronic Frontier Foundation, une organisation basée en Amérique – au début des années 1990, quand Internet devenait accessible dans le monde entier, « Le Net interprète la censure comme un dysfonctionnement et il la contourne5 ». On le sait aujourd'hui, c'était un mélange d'interprétation technique et d'optimisme forcé, un genre de vœu pieux doublé d'une prophétie autoréalisatrice.

JULIAN : Mais c'était vrai pour Usenet, un système de messagerie « many-to-many » (plusieurs-à-plusieurs) en quelque sorte, qui a vu le jour il y a une trentaine d'années. Pour expliquer simplement Usenet, imaginez qu'il n'y ait aucune distinction entre les individus et les serveurs et que chaque utilisateur possède son propre serveur Usenet. Vous écrivez quelque chose et vous l'envoyez à une ou deux personnes. Elles vérifient (automatiquement) qu'elles ne l'ont pas déjà. Si c'est le cas, elles le prennent et le transmettent à tous ceux avec qui elles sont connectées. Et ainsi de suite. Résultat : le message passe par tout le monde et tout le monde finit par en avoir une copie. Si quelqu'un cherche à censurer, on l'ignore, ça ne change rien. Le message se propage quand même grâce à tous ceux qui ne sont pas des censeurs. Gilmore parlait de Usenet, pas d'Internet. Il ne parlait pas non plus des pages Web.

ANDY : Sur le plan technique, c'est tout à fait vrai, mais l'interprétation de ses propos et leurs répercussions à long terme ont conduit à l'apparition de gens qui se considéraient comme étant eux-mêmes Internet. On a dit : « OK, il y a de la censure, nous la contournerons », alors que le politicien manquant de connaissances techniques pensait : « Eh merde, voici une nouvelle technologie qui restreint notre mainmise sur la sphère de l'information. » Alors je pense que Gilmore, qui a été l'un des penseurs importants du cypherpunk, a très bien réussi son coup en engageant les choses dans cette voie, ça a inspiré toute cette façon crypto-anarchique de posséder son propre moyen de communication anonyme sans crainte d'être pisté.

JÉRÉMIE : Je vois une différence dans ce que nous décrivons comme la propagation de la technologie, parce que, dans le cas du moulin comme de l'imprimerie, il fallait voir l'outil pour comprendre son fonctionnement, alors que nous tendons de plus en plus à intégrer le contrôle au sein même de la technologie. Le contrôle est intégré. Quand on regarde un ordinateur moderne, le

plus souvent, on ne peut même pas l'ouvrir pour en connaître tous les composants. Et tous les composants sont mis dans de petites boîtes – on ne peut pas savoir ce qu'ils fabriquent.

ANDY : À cause de la complexité ?

JÉRÉMIE : À cause de la complexité, mais aussi parce que la technologie elle-même n'est pas destinée à être comprise. C'est le cas de la technologie propriétaire6. Cory Doctorow en a fait la description dans « The War on General-Purpose Computing7 ». Quand l'ordinateur est une machine générique, on peut tout faire avec. On peut traiter toute information comme un input et la transformer en ce qu'on veut en tant qu'output. Cependant, nous avons de plus en plus tendance à fabriquer des machines qui sont des ordinateurs à tout faire, mais bridés pour ne servir qu'en tant que GPS, ou téléphone ou lecteur MP3. Nous construisons de plus en plus de machines dotées d'un contrôle intégré, pour interdire à l'utilisateur de faire certaines choses avec.

JULIAN : Ce contrôle intégré sert à empêcher les gens de comprendre la machine et de la détourner de l'emploi auquel la destine le fabricant, mais c'est pire aujourd'hui, parce qu'elle est connectée au réseau.

JÉRÉMIE : Oui, alors elle peut contenir une fonction de surveillance de l'utilisateur et de ses données. C'est la raison pour laquelle les logiciels gratuits sont si importants pour une société libre.

ANDY : Je suis tout à fait d'accord qu'il faut des machines à tout faire, mais ce matin, dans l'avion qui devait m'amener de Berlin, le décollage a été littéralement annulé – c'est la première fois que ça m'arrive. L'avion s'est rangé sur le côté et le commandant de bord a dit : « Mesdames et messieurs, à la suite d'une défaillance du système électrique, nous allons éteindre les systèmes et les redémarrer. » Je me suis dit : « Merde alors, c'est comme si on redémarrait Windows, Control Alt Suppr – peut-être que ça marche ! » Alors, en fin de compte, je ne serais pas forcément mécontent que l'avion soit équipé d'une machine spécialisée qui ne fait qu'une chose mais qui le fait très bien. Si je me trouve à bord d'un engin volant, je n'ai pas envie que les pilotes fassent des parties de Tetris ou que le système soit infecté par Stuxnet ou un truc dans le genre8.

JÉRÉMIE : L'avion ne traite pas tes données personnelles, il n'a pas prise sur ta vie.

ANDY : Ben, à vrai dire, un engin volant a quand même prise sur ma vie, pendant un moment.

JACOB : On peut parfaitement décrire l'argument de Cory, à mon avis, en disant qu'il n'y a plus de

voitures, plus d'avions, plus d'appareils auditifs, il y a des ordinateurs à quatre roues, des ordinateurs volants et des ordinateurs qui t'aident à entendre. Et la question n'est pas tant de savoir si ce sont des ordinateurs spécialisés ; c'est de savoir si on peut vérifier qu'ils font ce qu'ils prétendent faire, et si on peut évaluer qu'ils le font bien ou pas. Les gens disent souvent qu'ils ont le droit de verrouiller tout ça et de garder le secret, et ils fabriquent des ordinateurs complexes qu'ils truffent d'obstacles juridiques pour ceux qui chercheraient à les comprendre. Ça, c'est dangereux pour la société parce que rien ne garantit que tout le monde agit toujours dans l'intérêt commun, et on sait par ailleurs que l'erreur est humaine – et pas forcément mal intentionnée –, alors il est très dangereux de mettre tout ça sous les verrous pour toutes sortes de raisons, dont la moindre n'est pas que nous sommes tous imparfaits. C'est un fait. La possibilité d'accéder aux plans des systèmes qui sous-tendent notre existence est l'une des raisons pour lesquelles les logiciels libres sont si importants, mais cela vaut aussi pour le hardware libre. Cela augmente notre capacité de réaliser librement des investissements substantiels, d'améliorer les systèmes que nous utilisons et de déterminer si ces systèmes fonctionnent de la façon attendue.

Mais quoi qu'il en soit de la liberté, c'est aussi la raison pour laquelle il est important de comprendre ces systèmes, parce que, quand on ne les comprend pas, on tend à s'en remettre à une autorité, qu'il s'agisse de ceux qui comprennent ou de ceux qui sont capables de les contrôler sans être forcément à même de les comprendre. C'est pour cela qu'on assiste à un tel foin à propos de la cyberguerre – des gens apparemment autorisés en matière de guerre se mettent à parler de technologie comme s'ils savaient de quoi ils parlent. Ce genre d'individu parle sans arrêt de cyberguerre et pas un, pas un seul, ne parle de consolidation de la cyberpaix ou de quoi que ce soit de relatif à la consolidation de la paix. Ils ne parlent que de guerre parce que c'est leur business et ils s'efforcent de contrôler les processus technologiques et juridiques comme un moyen de promouvoir leurs propres intérêts. Alors quand nous n'avons aucun contrôle sur nos technologies, ces gens tentent de s'en servir à leurs fins, la guerre en particulier. Cette formule peut conduire à des choses franchement effrayantes – c'est d'ailleurs à mon avis ce qui nous a valu Stuxnet – et il y a des gens, par ailleurs raisonnables, pour suggérer, alors que les États-Unis sont en guerre, que ce genre de tactique est censée prévenir la guerre. L'argument est peut-être raisonnable pour un pays qui n'est pas activement en train d'en envahir d'autres, mais peu crédible quand il est développé au sein d'une nation impliquée dans plusieurs invasions.

1. Il s'agit de la manifestation du 6 avril 2008 contre la répression des ouvriers du textile en grève d'El-Mahalla El-Koubra. Peu avant la grève, le Mouvement de la jeunesse du 6-Avril s'était constitué en tant que groupe sur Facebook pour appeler les Égyptiens à manifester au Caire et ailleurs en convergence avec l'action menée à El-Mahalla. Les manifestations n'ont pas abouti et les administrateurs du groupe Facebook, Israa Abdel Fattah et Ahmed Maher, ont été arrêtés. Maher a été torturé pour obtenir son mot de passe Facebook. Le Mouvement de la jeunesse du 6-Avril a ensuite joué un rôle dans la révolution égyptienne de 2011. Voir « Cairo Activists Use Facebook to Rattle Regime », Wired, 20 octobre 2008 : http://www.wired.com/techbiz/startups/magazine/16-11/ff_facebookegypt?currentPage=all (lien vérifié le 25 novem- bre 2012).

2. « Comment manifester intelligemment », auteurs anonymes, distribué au début des dix-huit jours du soulèvement qui a fait tomber Hosni Moubarak (arabe) : http://www.itstime.it/Approfondimenti/Egyptian Revolution Manual.pdf. Des extraits du document ont été traduits en anglais et publiés sous le titre « Egyptian Activists' Action Plan: Translated », The Atlantic, 27 janvier 2011 : http://www.theatlantic.com/international/archive/2011/01/ egyptian-activists-action-plan-translated/70388 (les deux liens ont été vérifiés le 25 novembre 2012).

3. Le panoptique est un modèle de prison conçu en 1787 par le philosophe Jeremy Bentham, où un seul gardien peut secrètement surveiller tous les détenus à la fois grâce à la perspective visuelle que lui offre la disposition des lieux. Jeremy Bentham (édité par Miran Bozovic), The Panopticon Writings (Verso, 1995), disponible en ligne : http://cartome.org/panopticon2.htm (lien vérifié le 25 novembre 2012).

4. Johannes Gutenberg (vers 1398-1468) est un orfèvre allemand qui inventa le caractère mobile d'imprimerie typographique, qui donnera lieu à certains des principaux bouleversements sociaux de l'histoire. L'invention de la presse d'imprimerie est l'événement historique le plus similaire à l'invention d'Internet.

5. John Gilmore est l'un des cypherpunks de la première heure, l'un des fondateurs de l'Electronic Frontier Foundation et un activiste des libertés publiques. La phrase que cite Andy a été reprise pour la première fois dans : « First Nation in Cyberspace », Time Magazine, 6 décembre 1993. Voir le site de John Gilmore : http://www.toad.com/gnu (lien vérifié le 25 novembre 2012).

6. « Les technologies propriétaires sont tout type de système, d'outil ou de procédé technique développé par et pour une entreprise spécifique... [L]es idées développées et soumises par les employés sont généralement considérées comme appartenant à l'employeur, ce qui en fait des technologies propriétaires », définition empruntée à wiseGEEK : http://www.wisegeek.com/what-is-proprietary-technology.htm (lien vérifié le 26 novembre 2012).

7. Cory Doctorow, « The coming war on general-purpose computing » (La guerre imminente contre l'informatique généraliste), Boing Boing, 10 janvier 2012 (tiré d'un discours liminaire prononcé devant le Chaos Computer Congress en décembre 2011) : http://boingboing.net/2012/01/10/lockdown.html (lien vérifié le 26 novembre 2012).

8. Stuxnet est un ver informatique extrêmement sophistiqué dont on attribue l'élaboration aux États-Unis et à Israël dans le but de s'en prendre au matériel Siemens prétendument employé par l'Iran pour enrichir l'uranium. Pour une description générale de Stuxnet, voir : http://fr.wikipedia.org/wiki/Stuxnet.

Voir aussi « WikiLeaks: US advised to sabotage Iran nuclear sites by German thinktank », The Guardian, 18 janvier 2011 : http://www.guardian.co.uk/world/2011/jan/18/wikileaks-us-embassy-cable-iran-nuclear.

WikiLeaks a publié l'une des premières descriptions des effets attribués à Stuxnet – l'accident nucléaire survenu dans les installations iraniennes de Natanz. Voir « Serious nuclear accident may lay behind Iranian nuke chief's mystery resignation », WikiLeaks, 17 juillet 2009 :

http://wikileaks.org/wiki/Serious_nuclear_accident_may_lay_behind_Iranian_nuke_chief%27s_mystery_resignation.

Certaines fuites de l'entreprise de renseignement mondial Stratfor, rendues publiques par WikiLeaks, laissent soupçonner une implication israélienne. Voir Email ID 185945, The Global Intelligence Files : http://wikileaks.org/gifiles/docs/185945_re-alpha-s3-g3-israel-iran-barak-hails-munitions-blast-in.html (liens vérifiés le 26 novembre 2012).

Militarisation du cyberespace

JULIAN : Je constate qu'il y a aujourd'hui une militarisation du cyberespace, au sens d'une occupation militaire. Quand on communique sur Internet, quand on communique par un téléphone portable, qui est aujourd'hui raccordé à Internet, ces communications sont interceptées par des services de renseignements militaires. C'est comme si on avait un tank dans sa chambre à coucher. C'est un soldat qui s'installe entre toi et ta femme quand vous vous envoyez des SMS. En matière de communications, nous vivons tous sous la loi martiale, c'est juste que les tanks ne se voient pas – mais ils sont bien là. En ce sens, Internet, qui était censé constituer un espace civil, est devenu un espace militarisé. Mais Internet est notre espace, parce que nous l'utilisons tous pour communiquer entre nous et avec nos familles. Les communications qui constituent le cœur même de notre vie privée circulent aujourd'hui sur Internet. De fait, nos vies privées sont entrées dans une zone militarisée. C'est comme si on avait un soldat sous le lit. C'est une militarisation de la vie civile.

JACOB : Juste avant de venir ici, on m'a demandé d'être l'entraîneur de l'équipe du Security and Privacy Research Laboratory de l'université de Washington lors de la compétition Pacific Rim Collegiate Cyber Defense. On m'a appelé à la dernière minute pour jouer les conseillers. On a donné de notre temps pour participer à une simulation de cyberguerre où le SPAWAR, un bras civil de l'US Navy qui entre autres met au point des tests d'intrusion et s'occupe aussi bien de piratage informatique offensif que de piratage informatique défensif, a tenu le rôle de ce qu'on appelle habituellement l'équipe Rouge1. Le but des Rouges est d'attaquer tous les autres joueurs et chacun doit défendre le système informatique qui lui a été confié au début de l'événement sans qu'il en sache quoi que ce soit à l'avance. On ne sait pas quel type de système on va devoir défendre et on ne sait même pas trop au début comment on compte les points, alors on ne peut que faire de son mieux en espérant que ça se passera bien.

JULIAN : Tu es bien sûr qu'il s'agit d'un jeu ? Peut-être que ce n'en est pas un !

JACOB : Non, on te donne un tas d'ordinateurs et tu dois les protéger contre des adversaires qui cherchent à pénétrer dans le système et à s'en emparer. C'est comme une version pour enfants du jeu du drapeau dans une vraie conférence de hackers ou un truc dans le genre, et c'est intéressant, parce que les types ont beaucoup de moyens, ils ont écrit des logiciels2.

JULIAN : Mais quel est le but – du point de vue de l'US Navy ?

JACOB : S'ils parrainent ça, c'est pour former les cyberguerriers de demain, alors je vous ai par exemple apporté un bloc-notes de la CIA parce qu'elle était là pour recruter. Il y avait un type nommé Charlie – Charlie, de la CIA – qui expliquait que si jamais on voulait rejoindre les rangs de la CIA, c'était une fabuleuse occasion de travailler dans le monde réel. Et il y avait les gens du SPAWAR et de Microsoft qui recrutaient aussi. L'idée, c'était de former tous ces gens, toutes ces équipes, pour qu'ils participent au championnat national, qu'ils aient envie de gagner, de « défendre la nation », puis d'être capables aussi de se mettre à faire du piratage offensif, comme des cyberguerriers, pas des cyberdéfenseurs. On a obtenu un score de 4 000 points, ce qui équivaut à peu près au total des différents scores des équipes arrivées deuxième, troisième et quatrième. On était largement au-dessus de la mêlée.

JULIAN : Allez, allez, allez !

JACOB : Je n'y suis pour rien – mon discours de motivation a dû se résumer à un truc du genre « Eh, après la pluie vient... l'orage », je ne suis pas particulièrement doué pour le coaching – et ces types sont juste très forts. Mais c'était intéressant, parce que tout se passait dans un cadre guerrier, alors ils disaient : « Eh, on veut entendre ton cri de guerre ! » Et moi : « Plaît-il ? » C'est ce qu'ils disaient au déjeuner, par exemple, quand on a arrêté de défendre nos systèmes pendant la pause. Ils voyaient tout en termes de systèmes d'attaque et de guerre et de cyberguerre et ils trouvaient ça formidable. Mais le truc intéressant, c'est que j'ai eu l'impression que beaucoup de gars, et pas seulement dans l'équipe que j'entraînais, renâclaient parce que ce n'était pas le noble art de la guerre qu'on leur enseignait – ça ressemblait plus à une compétition d'administrateurs systèmes – et cela leur paraissait tout bonnement dégueulasse3. C'était vraiment bizarre, parce qu'il y avait tous ces types qui venaient du milieu de la guerre, ils avaient une perspective guerrière, mais ils n'enseignent pas la stratégie, ils étaient braqués sur une rhétorique de défense ou d'attaque des systèmes, et ils y mêlaient tellement de considérations guerrières qu'ils étaient en train d'énerver tout le monde pour tenter de leur transmettre une espèce de ferveur patriotique. Ils ne promouvaient pas la pensée créative ou un cadre de travail favorisant l'analyse indépendante ; ils encourageaient une mentalité de rouage, celle du type qui obéit aux ordres pour le bien de la nation. Je n'avais jamais vu ça. Ça me rendait malade, et l'essentiel de mon équipe a eu du mal à l'avaler ou même à le prendre au sérieux.

JULIAN : Tu crois que c'est l'entraînement de base de l'US Navy qu'ils ont juste transposé à un autre domaine ? Est-ce qu'il s'agit d'une démarche qui vient du sommet de la hiérarchie – d'une décision de stratégie internationale – de la part des États-Unis ?

ANDY : C'est plus comme les nazis, avec leurs camps de jeunesse où ils endoctrinaient les enfants.

JACOB : Sie können das sagen weil du bist Deutsche. Tu peux te permettre de dire ça parce que tu es allemand. Non, ce n'est pas ça. L'implication de l'US Navy tient simplement au fait que l'État américain sponsorise tout ça. Ils m'ont demandé de diriger une équipe parce qu'ils avaient besoin de quelqu'un pour le faire, et j'ai accepté parce que j'aimais bien les types qui y participaient, les étudiants. En vérité, ça se résume au fait que le gouvernement américain est vraiment en train d'essayer de convaincre des gens de se consacrer à ça et qu'ils le font dans une perspective nationaliste. C'est très, très bizarre d'y participer parce que, d'un côté, il est bon de savoir comment protéger son système et il est bon de comprendre toute l'infrastructure sur laquelle repose notre existence ; mais, d'un autre côté, ils ne cherchaient pas à aider les gens à comprendre, ils cherchaient à faire monter la mayonnaise d'une certaine ferveur pour qu'ils soient heureux d'accomplir ce genre de tâche.

ANDY : Malheureusement, les États-Unis n'ont que très peu intérêt à ce que les systèmes soient sûrs, ils préfèrent qu'ils soient vulnérables pour mieux pouvoir en prendre le contrôle. Leur volonté de contrôler le cryptage partout dans le monde ne va pas aussi loin qu'au début, vers 1988, quand le sous-secrétaire américain au Commerce pour les échanges internationaux, David Aaron, avait fait une tournée mondiale en proclamant que l'État devait avoir accès aux clés de cryptage de tout le monde4. Mais le cryptage est toujours considéré comme une technologie à double usage, et son exportation sous forme de produits grand public vers de nombreux pays est limitée légalement, avec l'accord du monde entier, par le prétendu Arrangement de Wassenaar5. Cela peut paraître raisonnable dans un contexte où l'on décrète que certains pays et leurs actes incarnent « le mal », mais ça montre bien à quel point il y a deux poids deux mesures, puisque la technologie de surveillance des télécommunications, elle, n'est à ce jour limitée par aucun contrôle à l'exportation6.

JULIAN : Andy, tu as passé des années à concevoir des téléphones cryptographiques. Quel type de surveillance de masse est en cours dans les télécommunications ? Dis-moi quel est le travail de pointe en ce qui concerne le renseignement d'État et l'industrie de la surveillance de masse ?

ANDY : C'est le stockage de masse – c'est-à-dire qu'on stocke toutes les télécommunications, tous les appels vocaux, toutes les données de trafic, tous les usages du Short Message Service (SMS), mais aussi les connexions Internet, et dans certaines situations au moins les mails. Si on compare le budget militaire au coût de la surveillance et à celui des cyberguerriers, les systèmes d'armement normaux coûtent beaucoup d'argent. Les cyberguerriers ou la surveillance de masse sont très peu coûteux si on les compare au prix d'un avion. Un avion militaire coûte dans les...

JULIAN : Environ 100 millions de dollars.

ANDY : Et le coût du stockage baisse d'année en année. À vrai dire, on a fait quelques calculs avec le Chaos Computer Club : on peut stocker avec une qualité de voix correcte tous les appels

téléphoniques allemands échangés pendant un an pour environ 30 millions d'euros tout compris, avec les frais administratifs généraux, et là-dedans le stockage pur représente environ 8 millions d'euros7.

JULIAN : Et il existe même des entreprises comme VASTech, en Afrique du Sud, qui vendent ces systèmes pour 10 millions de dollars par an8. « Nous interceptons tous vos appels, nous stockons tous les appels interceptés. » Mais on est passé depuis quelques années de l'interception de tout ce qui transite d'un pays à un autre, en ciblant les individus qu'on veut surveiller et en leur assignant des contrôleurs humains, à l'interception et au stockage d'absolument tout, et de façon définitive.

ANDY : Pour faire un historique rapide, autrefois, on était ciblé parce qu'on occupait une certaine position diplomatique, parce qu'on travaillait avec telle ou telle entreprise, parce qu'on était soupçonné de faire quelque chose ou qu'on était en contact avec quelqu'un qui faisait quelque chose, et des mesures de surveillance étaient alors prises. Aujourd'hui, on trouve beaucoup plus efficace de dire : « On ramasse tout et on fera le tri après. » Alors ils utilisent le stockage à long terme, et pour décrire les deux branches du secteur, on parle généralement d'approche « tactique » ou d'approche « stratégique ». Tactique, ça veut dire : « Maintenant, à cette réunion, il faut faire entrer quelqu'un avec un micro, avec une veste équipée ou disposer de systèmes de surveillance GSM actifs dans une voiture, capables d'intercepter tout ce qui se dit sur-le-champ, sans avoir à intervenir auprès de l'opérateur réseau, obtenir un mandat de perquisition ni quoi que ce soit de ce genre, pas de procédure légale, il n'y a qu'à le faire. » L'approche stratégique est de le faire par défaut, on enregistre tout, et on fait le tri plus tard à l'aide de systèmes d'analyse.

JULIAN : Alors l'interception stratégique, ça consiste à prendre tout ce que relaie un satellite de communication, tout ce qui passe dans un câble de fibre optique.

ANDY : Parce qu'on ne sait jamais qui peut être suspect.

JACOB : Il y a une affaire aux États-Unis qu'on a appelé l'affaire NSA/AT&T – et notamment le deuxième procès : Hepting contre AT&T. À Folsom, en Californie, Mark Klein, un ancien technicien pour le compte du géant des télécommunications AT&T, a révélé que la NSA, la National Security Agency américaine, s'emparait de toutes les données qu'AT&T voulait bien lui remettre. Ils prenaient tout, en vrac – données et appels vocaux –, si bien que chaque fois que j'ai décroché le téléphone à San Francisco dans la période indiquée par Mark Klein, on sait que la NSA, sur le sol américain, contre des citoyens américains, interceptait tout9. Je suis à peu près certain qu'ils ont utilisé ces données interceptées dans les enquêtes portant sur des individus aux États-Unis, ce qui soulève d'intéressantes questions de constitutionnalité parce qu'ils conservent ces données pour toujours.

JÉRÉMIE : Il y a aussi l'exemple d'Eagle, le système vendu par l'entreprise française Amesys à la

Libye de Kadhafi, dont la notice de présentation comportait l'expression « mécanisme d'interception à l'échelon national ». C'est une grosse boîte qu'on installe quelque part et qui permet d'écouter les conversations de tout un peuple10.

JULIAN : Il y a dix ans, on prenait tout ça pour du fantasme, pour un truc auquel seuls pouvaient croire les esprits paranoïaques, mais les coûts de l'interception massive ont baissé au point qu'un pays comme la Libye, doté de moyens relativement limités, pouvait s'y livrer avec du matériel français. En fait, pour ce qui est de l'interception, la plupart des pays en sont là. Le prochain grand bond portera sur l'efficacité de la compréhension de ce qui est intercepté et stocké et de la réaction qui suit. Beaucoup de pays pratiquent aujourd'hui l'interception stratégique de tout le trafic entrant et sortant, mais pour ce qui est des actions à entreprendre par la suite, comme le blocage automatique de comptes bancaires, le déploiement de policiers, la marginalisation de certains groupes ou l'émancipation d'autres, on est encore en phase de transition. Siemens propose aux agences de renseignements une plateforme qui produit des actions automatisées : lorsque la cible A se trouve à au moins un certain nombre de mètres de la cible B, selon les données d'interception de leur téléphone portable, et que la cible A reçoit un mail où il est fait mention d'une certaine chose – un mot clé –, une action est déclenchée. C'est en route.

1. En ingénierie de la sécurité, les tests d'intrusion sont la désignation d'attaques que l'on porte de façon légale et autorisée contre un système ou un réseau informatique, comme le ferait un utilisateur non autorisé, de façon à en éprouver le niveau de sécurité. Les chercheurs en sécurité sont souvent recrutés dans la communauté des pirates pour conduire des tests d'intrusion sur des systèmes sécurisés.

2. Le jeu du drapeau est à l'origine un jeu d'extérieur impliquant deux équipes, chacune tenant une position et protégeant un drapeau. L'objectif est de s'emparer du drapeau de l'équipe adverse et de le rapporter dans son camp. Dans les conférences de pirates, on joue à une version informatique de ce jeu dans laquelle les équipes attaquent et défendent des ordinateurs et des réseaux.

3. Sysadmin Cup est une contraction de System Administrator Cup. Un administrateur système est une personne qui travaille dans les technologies de l'information, qui entretient et opère un système ou un réseau informatique. Ce que Jacob veut dire, c'est que l'exercice ressemblait à un tournoi d'administrateurs systèmes.

4. « Aaron says encryption protects privacy, commerce », US Information Service, Washington, 13 octobre 1998 : http://www.fas.org/irp/news/1998/10/98101306_clt.html (lien vérifié le 27 novembre 2012).

5. Site de l'Arrangement de Wassenaar : http://www.wassenaar.org (lien vérifié le 27 novembre 2012).

6. Andy fait ici allusion à plusieurs faits survenus pendant les « premières guerres du cryptage » des années 1990. Quand les activistes cypherpunks se sont mis à disséminer des outils cryptographiques puissants sous forme de logiciels gratuits, l'administration américaine a pris des mesures pour faire entrave à leur bonne utilisation. Elle a classé la cryptographie au registre des munitions et restreint son exportation ; elle a essayé d'introduire des technologies concurrentes délibérément cassées de façon que les forces de l'ordre soient toujours en mesure de décrypter les informations ; et elle a essayé d'introduire la combine controversée de l'« autorité de séquestre ». Pendant un petit moment après le tournant du siècle, tout le monde reconnaissait que ces efforts avaient largement échoué. Mais une « seconde guerre du cryptage » est bien en cours à présent, et on assiste à des tentatives législatives et techniques de prendre à revers l'usage de la cryptographie, ou de la marginaliser d'une façon ou d'une autre.

7. Ce calcul correspond aux 196,4 milliards de minutes de communications des téléphones fixes en Allemagne en 2010, numérisées avec un codec vocal de 8 Kbps, ce qui donne un total de 11 784 pétaoctets (Po), qu'on a arrondis à 15 Po. En admettant que le stockage brut coûte 500 000 dollars par Po, cela représente 7,5 millions de dollars, ou environ 6 millions d'euros. À quoi s'ajoutent les coûts d'une installation correcte de centrale de données, la puissance de traitement, les connexions et la main-d'œuvre. Même si on y ajoute les 101 milliards de minutes de la téléphonie mobile en Allemagne en 2010, soit 50 Po et 18,3 millions d'euros supplémentaires, c'est encore beaucoup moins cher qu'un seul avion militaire comme l'Eurofighter (90 millions d'euros) ou le F22 (150 millions de dollars).

8. Pour en savoir plus à propos de VASTech, voir buggedplanet : http://buggedplanet.info/index.php?title= VASTECH (lien vérifié le 27 novembre 2012).

9. Le scandale de la surveillance intérieure de la NSA est la plus importante affaire de surveillance massive de l'histoire des États-Unis. En vertu du Foreign Intelligence Surveillance Act (FISA) de 1978, les agences américaines n'ont pas le droit d'espionner des citoyens américains sans mandat. Après le 11-Septembre, la NSA a massivement enfreint le FISA, grâce à un ordre administratif secret de George W. Bush. L'administration Bush a revendiqué l'autorité exécutive d'agir de la sorte au titre des lois d'urgence de 2001 approuvées par le Congrès : l'Authorization for Use of Military Force (AUMF) et le Patriot Act. Le programme d'espionnage intérieur sans mandat – qui a profité de la collaboration d'entreprises privées, dont AT&T – est resté secret jusqu'en 2005, date de sa révélation par le New York Times. Voir « Bush Lets U.S. Spy on Callers Without Courts », New York Times, 16 décembre 2005 : http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all.

Les journalistes du New York Times avaient été contactés par un lanceur d'alerte anonyme qui les avait informés de l'existence de ce programme de surveillance sans mandat. En 2004, le directeur de la rédaction, Bill Keller, avait accepté de ne pas sortir l'information avant un an à la demande de l'administration Bush, le temps que sa réélection soit acquise. En 2005, le New York Times s'est empressé de publier le papier quand il a appris que l'administration cherchait à obtenir une injonction de restriction préalable, similaire à celle de l'affaire des Pentagon Papers.

L'administration Bush a affirmé que le programme de la NSA n'avait rien d'illégal. Le département de la Justice a immédiatement lancé une enquête pour identifier la source de la fuite, mettant vingt-cinq agents fédéraux et cinq procureurs sur le coup. D'éminents dirigeants du Parti républicain ont réclamé que le New York Times soit poursuivi au titre de l'Espionage Act.

Dans le sillage de la publication de l'article par le New York Times, d'autres lanceurs d'alerte ont contacté la presse, dessinant peu à peu une image très détaillée de la violation des lois et du gaspillage pratiqués aux plus hauts niveaux de la NSA. Une foule de recours collectifs ont été déposés par des associations de défense des libertés comme l'American Civil Liberties Union (ACLU) et l'Electronic Frontier Foundation (EFF). Dans l'une de ces affaires, ACLU vs NSA, les plaignants n'ont même pas été admis à comparaître parce qu'ils n'avaient pas pu prouver qu'ils avaient été personnellement espionnés. Dans une autre, Hepting vs AT&T, un lanceur d'alerte d'AT&T, Mark Klein, a produit une déclaration sous serment révélant l'étendue de la coopération d'AT&T avec le programme d'espionnage intérieur. Voir la partie consacrée à Hepting vs AT&T sur le site d'EFF : https://www.eff.org/cases/hepting.

Mark Klein, ancien employé d'AT&T à Folsom, San Francisco, a témoigné au procès Hepting vs AT&T. Sa déclaration sous serment auprès de l'EFF a révélé l'existence de la « chambre 641A », qui abritait des installations d'interception stratégique opérée par AT&T pour le compte de la NSA. Les installations comportaient un accès aux troncs de fibre optique contenant le gros du trafic Internet, qui leur permettait de surveiller tout le trafic Internet transitant par l'immeuble, aussi bien national qu'international. Un autre lanceur d'alerte de la NSA, William Binney, a estimé qu'il devait exister une vingtaine d'installations de ce genre, toutes situées en des points stratégiques du réseau de télécommunications des États-Unis. La déclaration de Klein fournit aussi des informations importantes sur les caractéristiques du programme de surveillance de la NSA, confirmées par des lanceurs d'alerte de la NSA. C'est un cas d'« interception stratégique » – tout le trafic Internet qui traverse les États-Unis est copié et stocké indéfiniment. On sait avec certitude que le trafic intérieur des États-Unis est intercepté et stocké lui aussi, parce que d'un point de vue technique, quand on gère un tel volume de trafic, il est impossible de dissocier la part pour laquelle un mandat serait requis en vertu du FISA. Selon l'interprétation juridique officielle du FISA actuellement en cours, l'« interception » ne survient qu'au moment où une communication intérieure déjà interceptée et stockée par la NSA est « consultée » sur la base de données de la NSA, et ce n'est qu'à ce stade que le mandat est requis. Les citoyens américains peuvent donc considérer que l'ensemble de leur trafic de télécommunications (y compris les appels vocaux, les SMS, le courrier électronique et la navigation sur Internet) est surveillé et stocké pour toujours dans les centres de données de la NSA.

En 2008, réagissant au grand nombre de plaintes qui ont suivi le scandale des écoutes, le Congrès des États-Unis a voté des amendements à la loi FISA de 1978, immédiatement ratifiés par le président. Ces amendements ont préparé le terrain à l'octroi d'une « immunité rétroactive » très controversée contre toute poursuite pour non-respect du FISA. Le sénateur Barack Obama, pendant sa campagne présidentielle, avait fait de la « transparence » un de ses thèmes de prédilection et promis de protéger les lanceurs d'alerte, mais peu après sa prise de fonction, en 2009, son département de la Justice a maintenu la politique de l'administration Bush, et a fini par avoir gain de cause dans l'affaire Hepting et d'autres en accordant l'« immunité rétroactive » à AT&T.

Si l'enquête du département de la Justice sur l'identité de la source de l'article initial du New York Times n'a pas permis de retrouver le lanceur d'alerte, elle a permis d'en démasquer d'autres, qui avaient pris la parole après la parution de l'article. Parmi ceux-là se trouvait Thomas Drake, ancien cadre supérieur de la NSA, qui avait passé des années à se plaindre en interne auprès des commissions de surveillance du renseignement du Congrès (Congressional Intelligence Oversight Committees) de la corruption et du gaspillage en cours au sein du programme Trailblazer de la

NSA. Les plaintes en interne ont été supprimées, et tout fonctionnaire tenté de poursuivre cette voie a été écarté. Après l'article du New York Times, Drake avait livré le cas du programme Trailblazer au Baltimore Sun. À la suite de l'enquête d'un jury d'accusation, il a été mis en examen, désigné « ennemi de l'État » et inculpé au titre de l'Espionage Act. Voir « The Secret Sharer », New Yorker, 23 mai 2011 :

http://www.newyorker.com/reporting/2011/05/23/ 1105 23fa_fact_mayer?currentPage=all

L'accusation contre Drake s'est effondrée en juin 2011 après avoir été rendue publique, et après qu'on a tenté d'imposer à Drake un arrangement à l'amiable. Le département de la Justice a dû se contenter de le voir plaider coupable d'un seul délit mineur. Drake a été condamné à un an de prison avec sursis et mise à l'épreuve.

Les retombées du scandale de la surveillance par la NSA ne sont pas finies. L'ACLU conduit une action en justice pour contester la constitutionnalité des amendements au FISA de 2008, c'est l'affaire Amnesty et al. vs Clapper. Voir « FISA Amendment Act Challenge », ACLU, 24 septembre 2012 : http://www.aclu.org/national-security/amnesty-et-al-v-clapper.

Dans l'affaire Jewel vs NSA, l'EFF cherche à mettre fin aux activités de surveillance exercées sans mandat par la NSA. Le dossier a été retoqué en 2009, quand l'administration Obama a invoqué l'immunité pour cause de secret défense. Voir la page de l'EFF consacrée à Jewel vs NSA : https://www.eff.org/cases/jewel. Toutefois, la cour d'appel pour le neuvième circuit a autorisé la réouverture du dossier en décembre 2011. Thomas Drake et d'autres lanceurs d'alerte de la NSA, William Binney et J. Kirk Wiebe, apportent des éléments au dossier Jewel vs NSA. L'administration Obama – qui a été élue sur un programme de transparence – a poursuivi plus de lanceurs d'alerte au titre de l'Espionage Act que toutes les administrations préalables réunies (tous les liens de cette note ont été vérifiés le 28 novembre 2012).

10. Voir la page consacrée au système Eagle sur buggedplanet : http://buggedplanet.info/index.php? title= AMESYS#Strategic_.28.22Massive.22.29_Appliances (lien vérifié le 28 novembre 2012).

Combattre la surveillance totale

avec les lois humaines

JÉRÉMIE : C'est donc à présent un fait. La technologie permet la surveillance totale de toutes les communications. Et puis il y a l'autre aspect de la chose, ce qu'il convient de faire de tout ça. Admettons qu'il existe certains usages légitimes pour ce que vous appelez la surveillance tactique – les enquêteurs sur la piste de méchants et de réseaux de méchants pourraient avoir besoin, sous contrôle judiciaire, d'employer ce genre d'outils –, mais la question est de savoir où passe la ligne pour cette supervision judiciaire, où passe la ligne du contrôle citoyen de ces technologies. C'est une question politique. Quand on en arrive à ces questions politiques, on a des politiciens qui ne comprennent pas la technologie en jeu et à qui l'on demande simplement de signer quelque chose, et il me semble que nous, citoyens, avons un rôle à jouer, qui ne se limite pas à l'explication du fonctionnement général de la technologie, y compris aux politiciens, mais consiste aussi à intervenir

dans le débat politique autour de l'usage de ces technologies. Je sais qu'il y a eu en Allemagne un mouvement général contre la conservation systématique des données qui a abouti à l'annulation de la loi sur la conservation des données par la Cour constitutionnelle1. Un débat est en cours dans l'Union européenne à propos de la révision de la directive sur la conservation des données2.

ANDY : Ce que tu décris, c'est la théorie de l'État démocratique qui, évidemment, est bien obligé de filtrer ici et là quelques méchants individus et de mettre leur téléphone sur écoute à la suite d'une décision de justice et avec une supervision pour s'assurer que ce soit fait dans les règles. Le problème, c'est que les autorités doivent agir dans le cadre de la loi. Si elles ne le font pas, à quoi servent ces lois ? Plus particulièrement, avec cette approche stratégique, certains États démocratiques en Europe sont en train d'acheter en masse des machines qui leur permettent d'agir en marge de la loi en matière d'interception, parce qu'ils n'auront pas besoin d'une décision de justice, ils n'auront qu'à allumer la machine et le faire, et cette technologie échappe à tout contrôle.

JULIAN : Mais peut-on dire qu'il y a deux approches concernant la surveillance massive par les États – les lois physiques et les lois humaines ? L'une consiste à utiliser les lois de la physique en fabriquant des appareils qui empêchent l'interception. L'autre est d'établir des mécanismes de contrôle démocratique en légiférant pour s'assurer qu'un mandat soit indispensable et ainsi de suite pour obtenir un certain degré de responsabilité. Mais l'interception stratégique ne peut pas s'inscrire là-dedans, elle ne peut pas être significativement bridée par la réglementation. L'interception stratégique consiste à intercepter tout sans se soucier de savoir qui est innocent et qui est coupable. Il faut se rappeler que c'est le noyau dur de l'ordre établi qui exerce cette surveillance. Il y aura toujours un manque de volonté politique pour mettre au jour l'espionnage d'État. Et la technologie est intrinsèquement si complexe, et son usage est en pratique si secret, qu'il ne peut y avoir de réelle surveillance démocratique.

ANDY : Ou alors tu espionnes ton propre Parlement.

JULIAN : Mais ce sont des prétextes – la mafia et le renseignement étranger –, des prétextes que les gens vont accepter pour établir un tel système.

JACOB : Les quatre Cavaliers de l'Infocalypse : la pornographie infantile, le terrorisme, le blanchiment d'argent et la guerre contre certaines drogues.

JULIAN : Une fois qu'on a mis en place ce système de surveillance, compte tenu de sa complexité, compte tenu du fait qu'il est conçu pour opérer secrètement, n'est-il pas vrai qu'il ne peut pas être régulé par des mesures politiques ? Je crois qu'hormis dans certains pays tout petits comme l'Islande, à moins qu'il y ait une situation révolutionnaire, il n'est tout bonnement pas possible de contrôler par des lois et des mesures l'interception massive. Ça n'arrivera pas. Il est trop bon marché et trop facile de contourner toute responsabilité politique et de réaliser ces interceptions

malgré tout. Les Suédois ont adopté une loi sur l'interception en 2008, le FRA-lagen, en vertu de laquelle le FRA, l'agence suédoise de renseignements des signaux radiophoniques, pouvait légalement intercepter en bloc toute communication traversant le pays et l'envoyer aux États-Unis, avec quelques restrictions3. Mais comment voulez-vous faire respecter ces restrictions une fois que le système d'interception est en place et que l'organisation qui s'en occupe est une agence d'espionnage secrète ? C'est impossible. D'ailleurs, certaines affaires sont sorties, montrant que le FRA avait à plusieurs reprises enfreint la loi dans le passé. Beaucoup de pays le font tout simplement en dehors de la loi, sans aucune couverture légale. Alors on peut s'estimer heureux si, comme dans l'exemple suédois, ils décident que pour se prémunir contre toute poursuite, ils cherchent à se ranger dans la légalité en modifiant la loi. Et c'est ce qui arrive dans la plupart des pays – l'interception en bloc a lieu et, quand apparaît une proposition législative, c'est pour protéger les fesses de ceux qui s'y livrent.

Cette technologie est très complexe ; en Australie et au Royaume-Uni, par exemple, dans le débat qui a lieu autour de la proposition de loi visant à intercepter toutes les métadonnées, la plupart des gens ne comprennent pas bien ce que représentent les métadonnées, ni même le sens du terme4. Pour intercepter toutes les métadonnées, il faut bâtir un système qui intercepte physiquement toutes les données avant de tout mettre à la corbeille, sauf les métadonnées. Mais on ne peut pas faire confiance à un tel système. Il n'y a aucun moyen de déterminer s'il n'est pas en fait en train de tout intercepter et de tout stocker sans que des ingénieurs hautement qualifiés et dûment autorisés puissent vérifier précisément ce qui se passe, et la volonté politique pour créer un tel accès n'existe pas. Le problème est en train de s'aggraver parce que la complexité et le secret sont un mélange toxique. Lequel est occulté par sa complexité. Occulté par le secret. L'irresponsabilité est intégrée au système. C'est l'une de ses caractéristiques. Il est dangereux par sa conception même.

JÉRÉMIE : Je ne dis pas que l'approche par la réglementation peut fonctionner. Je dis juste que c'est en théorie comme ça que devrait fonctionner un système démocratique, et d'ailleurs, même dans cette théorie, les services secrets ont le droit d'outrepasser les règles qui valent pour la police et les enquêteurs ordinaires. Alors même si l'on encadrait correctement le comportement des enquêteurs ordinaires, d'autres pourraient encore utiliser ces technologies. Mais la question se pose vraiment de savoir s'il faut oui ou non réguler l'achat ou la possession de ces technologies plutôt que leur usage.

JULIAN : Ce sont des kits d'interception en bloc capables d'intercepter les communications de la moitié d'un pays ou d'une ville entière.

JÉRÉMIE : Oui. C'est comme l'arme nucléaire – ça ne se vend pas facilement, et certains pays peuvent chercher à en fabriquer eux-mêmes, mais ils se heurtent à des obstacles. Quand on parle de systèmes d'armement, c'est la technologie qui est régulée, pas l'usage qu'on en fait. Je crois que le débat pourrait porter sur le fait de savoir si ces technologies doivent ou non être considérées comme relevant du domaine de la guerre.

JACOB : Ça dépend. Quand ce sont des armes – et il ne fait aucun doute que le matériel de surveillance est une arme dans des pays comme la Syrie ou la Libye –, elles sont spécifiquement

employées pour cibler les gens sur un plan politique. L'entreprise française Amesys ciblait des individus au Royaume-Uni avec du matériel français dont l'utilisation serait illégale en France, et elle l'a vendu en connaissance de cause5.

ANDY : Et jamais ils ne feraient une chose pareille, n'est-ce pas ?

JACOB : Eh bien Amesys a été trahi par ses propres documents internes publiés dans les Spy Files6. Si l'on veut en parler en termes d'armement, il faut se souvenir que ce n'est pas comme si on vendait un camion à un pays. C'est comme si on lui vendait un camion, un mécanicien et une équipe dans le camion, qui cible sélectivement certaines personnes et leur tire dessus.

JULIAN : C'est comme vendre toute une flottille de camions.

ANDY : Le fait que la cryptographie soit soumise à régulation est intéressant. Il y a l'Arrangement de Wassenaar, d'application internationale, c'est-à-dire qu'on n'a pas le droit d'exporter de technologie de cryptage vers les pays déclarés « mal intentionnés » ou, pour une raison ou une autre, problématiques, ce qui va dans le sens de la protection contre la technologie de surveillance. Mais si tu vends du matériel de surveillance, tu peux vendre ces technologies à l'étranger. Il n'y a pas de restriction à l'exportation. Je dirais que cela tient simplement au fait que même les gouvernements démocratiques ont un intérêt propre, qui est de contrôler. Et même si l'on a affaire à des pays mal intentionnés et qu'on leur fournit du matériel de surveillance pour faire de vilaines choses, on en tirera profit, parce qu'on apprendra ce qu'ils écoutent, ce qu'ils redoutent, ou qui sont les principaux opposants au gouvernement du pays, ceux qui organisent des rassemblements politiques et ainsi de suite. Alors on sera en mesure de prédire la suite des événements, de parrainer certaines actions, etc. On est là au cœur du petit jeu sale qui se joue entre les pays, et c'est la vraie raison pour laquelle les systèmes de surveillance ne sont pas soumis à régulation.

JULIAN : Je voudrais pousser plus loin cette analogie entre la surveillance de masse et les armes de destruction massive. La possibilité de construire une bombe atomique est un fait physique et, une fois la bombe atomique construite, la géopolitique a changé, et avec elle la vie de beaucoup de gens – certains s'en sont trouvés mieux, d'autres au bord de l'apocalypse totale. Un mouvement de régulation a imposé des contrôles et, jusqu'à présent, ces contrôles nous ont préservés de la guerre nucléaire, exception faite du Japon. Mais il est aisé de savoir quand ces armes sont employées et quand elles ne le sont pas.

Avec la sophistication croissante de la surveillance de masse et la réduction de son coût survenues ces dix dernières années, on se trouve désormais au stade où la population double tous les vingt-cinq ans environ – alors que la capacité de surveillance double tous les dix-huit mois. La courbe de la surveillance dépasse celle de la population. Il n'y a pas d'issue. On en est aujourd'hui au point où 10 millions de dollars suffisent à acheter une unité pour stocker définitivement les interceptions massives d'un pays de taille moyenne. Alors je me demande s'il ne faut pas une réponse de même calibre. C'est vraiment une menace très lourde qui pèse sur la démocratie et sur la liberté dans le

monde entier et qui réclame une réponse, comme la menace de guerre atomique a imposé une réponse de grande envergure, pour tenter de la contrôler autant que possible.

ANDY : J'ai lu qu'en Libye les émeutiers du mouvement démocratique ont investi les stations de surveillance, où ils ont mis la main sur les archives et exhibé les preuves que les entreprises occidentales avaient soutenu la répression politique du régime de Kadhafi, et le nouveau gouvernement a repris telles quelles ces installations qui fonctionnent de nouveau aujourd'hui à plein régime7. Alors si je suis d'accord pour dire qu'il serait souhaitable de contrôler cette technologie, je suis un peu sceptique pour ce qui est de l'opposition entre les intérêts du citoyen et ceux des gens au pouvoir. Je ne dirais même pas qu'il s'agit forcément des gouvernements, parce que quiconque a la possibilité d'écouter toutes les conversations téléphoniques y gagne la possibilité de faire des choses. Ça concerne aussi la Bourse – en termes d'économie, il peut être très rentable d'être informé de ce qui se passe.

JULIAN : Dans les pays dotés de lois concernant ce qu'ont le droit de cibler les principales agences d'espionnage électronique – des agences comme la NSA aux États-Unis, le GCHQ (Government Communications Headquarters) britannique, le DSD (Defence Signals Directorate) en Australie –, on a modifié la législation pour y inclure le renseignement économique. Mettons par exemple que l'Australie et les États-Unis soient en lutte avec d'autres pays pour décrocher un marché de blé, ils espionneront tous ceux qui sont impliqués dans le marché. Il y a un moment que ça dure, et au moins dix ans que cela se sait – et il faut bien constater que ça passe puisqu'ils continuent à le faire. Ça a commencé avec le marché des armes, où des entreprises comme Lockheed Martin, Raytheon et Northrop ont conclu des accords, tout en participant à la construction de systèmes d'interception de masse parce que ces groupes ont des relations de copinage. Ils ont obtenu des faveurs de leurs amis et couvert l'interception de marchés d'armes au nom de la sécurité nationale. Mais cela s'applique à présent à tout ce qui peut profiter économiquement à un pays, autant dire à peu près tout.

JACOB : Lors du Chaos Communication Congress de décembre 2011, certains ont établi une bonne analogie en disant qu'il faudrait traiter la technologie de surveillance, surtout la technologie de surveillance tactique mais aussi la technologie de surveillance stratégique, à la façon des mines terrestres8. Je trouve que c'est une idée très forte. Un chemin est tracé mais cela ne veut pas dire qu'il faille l'emprunter, et donc que nous allions forcément vers la surveillance généralisée de chaque individu.

Même si certaines incitations économiques jouent contre nous. Quelqu'un m'a expliqué, par exemple, que l'ancien système téléphonique norvégien consistait essentiellement à faire tourner un compteur à vitesse variable selon que la destination d'un appel se trouvait près ou loin. Mais la compagnie de téléphone norvégienne n'avait pas le droit de conserver ou de constituer un registre des métadonnées des appels passés, comme le numéro qu'on avait composé, notamment à cause du souci du respect de la vie privée hérité de la Seconde Guerre mondiale. Il est donc possible de mettre au point cette technologie d'une telle façon qu'elle respecte la confidentialité, tout en s'accordant avec les fondamentaux de ce marché, et donc en étant économiquement avantageuse. De toute façon, nous ne pouvons pas gagner, par exemple avec les technologies GSM (mobiles). La façon dont ces systèmes sont aujourd'hui configurés, pas seulement en termes de facturation mais aussi d'architecture, ne permet pas de respecter la confidentialité, ni de la localisation ni du contenu.

JULIAN : Un téléphone portable est un mouchard qui peut aussi passer des appels.

JACOB : Tout à fait. Quand on dit que tous les habitants du tiers-monde sont espionnés, par exemple, qu'est-ce que cela signifie réellement ? Cela signifie que leur système téléphonique, qui constitue leur lien avec le reste du monde, est un dispositif d'espionnage dès que quelqu'un décide d'utiliser les données ainsi recueillies.

ANDY : J'ai vu que les pays africains sont en train d'obtenir toute une infrastructure Internet, avec fibre optique et commutateurs d'infrastructure, gracieusement offerte par les Chinois.

JACOB : Un cadeau de ZTE, ou quelque chose dans le genre9 ?

ANDY : Oui, et les Chinois sont évidemment très intéressés par ces données, alors ils ne demandent pas à être payés en argent, les données leur suffisent, c'est une nouvelle monnaie d'échange.

1. « German court orders stored telecoms data deletion », BBC, 2 mars 2010 : http://news.bbc.co.uk/1/hi/world/europe/8545772.stm (lien vérifié le 28 novembre 2012).

2. La directive 2006/24/CE du Parlement européen et du Conseil impose aux États européens de ne conserver les données des télécommunications des citoyens qu'entre six et vingt-quatre mois. C'est l'application de cette directive au droit allemand qui a été déclarée anti-constitutionnelle en Allemagne. En mai 2012, la Commission de l'Union européenne a traduit l'Allemagne devant la Cour européenne de justice pour ne pas s'être pliée à la directive (voir le communiqué de presse de la Commission : http://europa.eu/rapid/press-release_IP-12-530_fr.htm (lien vérifié le 28 novembre 2012).

3. Voir « Sweden approves wiretapping law », BBC, 19 juin 2008 : http://news.bbc.co.uk/1/hi/world/europe/ 7463333.stm.

Pour plus d'informations sur la loi FRA-lagen, voir Wikipédia : http://en.wikipedia.org/wiki/FRA_law (liens vérifiés le 28 novembre 2012).

4. Les métadonnées sont des « données sur les données ». Dans le contexte de cette discussion, les métadonnées désignent les données autres que le « contenu » des communications électroniques. C'est l'enveloppe plutôt que son contenu. La surveillance des métadonnées ne cible pas le corps des mails, mais plutôt toute l'information qui l'entoure – l'identité de l'expéditeur ou du destinataire, l'adresse IP (et donc la localisation) de l'émetteur, la date et l'heure de chaque courrier, etc. Toutefois, le fait est que la technologie permettant d'intercepter les métadonnées est la même que celle qui permet d'intercepter les contenus. Si vous accordez à quelqu'un le droit de surveiller vos métadonnées, son matériel interceptera forcément le contenu de vos communications. Par ailleurs, on ne se rend généralement pas bien compte que « les métadonnées prises ensemble sont elles-mêmes du contenu » – quand on rassemble toutes les métadonnées, on obtient une image d'une précision ahurissante des communications d'un individu.

5. Amesys appartient au groupe Bull, autrefois concurrent de la filiale allemande d'IBM, Dehomag, qui vendait des systèmes à cartes perforées aux nazis. Voir Edwin Black, IBM et l'Holocauste, Paris, Robert Laffont, 2001.

6. WikiLeaks a entrepris de rendre publics les Spy Files en décembre 2011, révélant l'étendue de la surveillance de masse. On peut y accéder : http://wikileaks.org/the-spyfiles.html.

7. Pour plus de détails, voir buggedplanet : http://buggedplanet.info/index.php?title=LY.

8. Le Chaos Communication Congress est un rassemblement annuel de hackers du monde entier organisé par le Chaos Computer Club.

9. Jacob parle de ZTE, l'un des deux producteurs chinois de matériel électronique (l'autre étant Huawei), très largement soupçonné de contenir une « porte dérobée ». Ce qu'il insinue, c'est que ce « cadeau » d'une infrastructure de communication a un prix – il sera, dans sa conception même, ouvert à la surveillance chinoise.

Espionnage par le secteur privé

JÉRÉMIE : La surveillance organisée par l'État est sans doute une question essentielle qui menace la structure même des démocraties et leur fonctionnement, mais il existe aussi une surveillance privée et la possibilité d'une collecte massive de données par le secteur privé. Il n'y a qu'à regarder Google. Si tu es un utilisateur ordinaire de Google, Google sait avec qui tu communiques, qui tu connais, ce que tu recherches, il connaît éventuellement ton orientation sexuelle et tes croyances

religieuses et philosophiques.

ANDY : Il en sait plus sur ton compte que toi-même.

JÉRÉMIE : Plus que ta mère en tout cas, et peut-être plus que toi-même. Google sait quand tu es en ligne et quand tu ne l'es pas.

ANDY : Sais-tu quelle recherche tu as accomplie il y a deux ans, trois jours et quatre heures ? Tu ne le sais pas ; Google si.

JÉRÉMIE : En vérité, j'essaie de ne plus utiliser Google pour ces raisons précises.

JACOB : C'est un peu le mouvement Kill your television, version XXIe siècle1. Une protestation très importante, sauf que l'effet de réseau empêche ton acte d'être efficace2. Tue ta télé, mec.

JÉRÉMIE : Ce n'est pas une protestation, en fait, c'est plus une façon de voir les choses.

ANDY : J'ai vu des films formidables où des gens jetaient leur téléviseur par la fenêtre du deuxième étage.

JÉRÉMIE : Ce n'est pas seulement la surveillance organisée par l'État, c'est la question de la confidentialité, la gestion des données par des tiers et la connaissance qu'ont les gens de ce qu'on fait de leurs données. N'étant pas utilisateur de Facebook, je n'y connais pas grand-chose. Aujourd'hui, avec Facebook, on voit des utilisateurs très heureux de livrer toutes sortes de données personnelles, mais peut-on reprocher aux gens de ne pas savoir où est la limite entre vie privée et vie publique ? Il y a quelques années, avant les technologies numériques, les gens qui avaient une vie publique étaient ceux qui travaillaient dans le show business, la politique ou le journalisme, et maintenant tout le monde peut avoir une vie publique en cliquant sur le bouton « publier ». Publier signifie rendre public, ça veut dire qu'on offre au reste du monde l'accès à cette donnée – et, évidemment, quand des adolescents envoient des photos où on les voit ivres ou un truc du genre, ils ne comprennent pas forcément que le monde entier y aura accès, possiblement pendant très, très longtemps. Facebook fait son beurre en brouillant la limite entre l'intimité, les amis et la publicité. Et il conserve même les données alors qu'on pense que ça ne concerne que les amis et les gens qu'on aime. Donc, quelle que soit la publicité qu'on entend donner à ses données, quand on clique sur « publier », on les remet d'abord à Facebook, qui les rend ensuite accessibles à certains autres usagers de Facebook.

JULIAN : Même la limite qui sépare État et entreprise est floue. Pour se faire une idée de l'expansion que connaît depuis dix ans le secteur des prestataires de services militaires en Occident, la NSA, qui est la plus grande agence d'espionnage du monde, travaillait avec seulement dix sous-traitants. Il y a deux ans, ils étaient plus de mille. La frontière entre ce qui relève de l'État et ce qui relève du privé est en train de s'estomper.

JÉRÉMIE : Et on peut discuter le fait que les agences d'espionnage américaines aient accès à toutes les données stockées par Google.

JULIAN : Mais c'est le cas.

JÉRÉMIE : Et aussi à toutes les données de Facebook, de sorte que Facebook et Google peuvent être une extension de ces agences.

JULIAN : As-tu eu droit à l'injonction de Google, Jacob ? Est-ce qu'une injonction a été envoyée à Google pour qu'ils livrent des informations relatives à ton compte ? WikiLeaks a reçu des injonctions chez Dynadot, l'hébergeur californien de son nom de domaine, où est déposée l'appellation wikileaks.org. Il y a eu des injonctions dans le cadre de l'enquête secrète menée par le jury d'accusation sur WikiLeaks, qui demandait des archives financières, des informations de login, etc., et il les a obtenues3.

JACOB : Selon le Wall Street Journal, Twitter, Google et Sonic.net, trois services que j'utilise ou que j'ai utilisés dans le passé, ont reçu une notification 2703(d), qui est une ordonnance d'injonction inhabituelle, notamment parce qu'elle doit rester secrète4.

JULIAN : En vertu du Patriot Act ?

JACOB : Non. Il s'agit essentiellement du Stored Communications Act (loi sur la conservation des communications). Ce que raconte le Wall Street Journal, c'est que chacun de ces services affirme que l'État lui a réclamé les métadonnées, et l'État a affirmé qu'il avait le droit de le faire sans mandat. Un procès est en cours qui décidera si l'État a le droit de garder le secret sur ses tactiques, pas seulement à l'égard du public, mais de la justice elle-même. J'ai appris tout ça en lisant le Wall Street Journal, comme tout le monde.

JULIAN : Alors Google fait de la lèche au gouvernement américain dans l'enquête du jury d'accusation sur WikiLeaks quand celui-ci requiert tes données par injonction – pas une injonction normale, un genre d'injonction des services secrets. On sait qu'en 2011 Twitter avait reçu un certain nombre d'injonctions de la part du même jury d'accusation, mais Twitter s'est battu pour pouvoir avertir les personnes dont les comptes étaient concernés – pour que l'ordonnance de non-publicité soit levée. Je n'ai pas de compte Twitter, alors je n'ai rien reçu, mais mon nom et celui de Bradley Manning figuraient sur toutes les injonctions parmi les informations requises. Jacob, comme tu avais un compte chez eux, Twitter a reçu une injonction te concernant. Google a reçu une injonction aussi, mais ils ne se sont pas battus pour pouvoir en informer le public5.

JACOB : C'est ce qu'on dit. C'est ce que j'ai lu dans le Wall Street Journal. Je n'ai peut-être même pas le droit d'y faire allusion autrement qu'en rapport avec le Wall Street Journal.

JULIAN : Parce que ces ordonnances ont aussi une clause de non-publicité ? Mais ça a été déclaré anticonstitutionnel, non ?

JACOB : Peut-être pas. Dans le cas de Twitter, il est de notoriété publique que nous avons perdu sur la requête à surseoir dans laquelle on argumentait que livrer ces données à l'État serait un préjudice irréparable puisqu'une fois qu'ils les auront, ce sera pour toujours. Ils ont dit : « Certes, mais votre requête est rejetée, Twitter doit livrer ces données. » L'appel est en cours, notamment sur le caractère secret de l'injonction – ça, je n'ai pas le droit d'en parler – mais, pour l'instant, la cour a statué que, sur Internet, il n'y a pas de confidentialité à partir du moment où on confie volontairement des informations à un tiers, et, soit dit en passant, sur Internet, tout le monde est un tiers.

JULIAN : Même si l'entreprise, qu'il s'agisse de Facebook ou Twitter, dit qu'elle préservera la confidentialité des informations.

JACOB : Bien sûr. Et c'est là que se situe la ligne floue entre l'État et l'entreprise. C'est sans doute l'élément le plus important à prendre en considération ici, le fait que la NSA et Google sont partenaires en matière de cybersécurité pour des raisons de défense nationale des États-Unis.

ANDY : Quelle que soit la définition de la cybersécurité dans ce contexte. Le terme est vaste.

JACOB : Ils cherchent à s'exempter totalement du Freedom of Information Act (loi pour la liberté d'information) pour pouvoir garder le secret. Et puis l'État américain affirme aussi qu'il a le droit d'émettre une injonction administrative, moins forte qu'un avis de recherche, et qui prévoit que le

tiers n'a pas le droit de vous en parler, que vous n'avez pas le droit de vous battre parce que c'est le tiers qui est directement impliqué, et le tiers n'a pas non plus de fondement constitutionnel pour protéger vos données.

JULIAN : Le tiers étant ici Twitter, Facebook ou le fournisseur d'accès.

JACOB : Ou n'importe qui d'autre. Ils ont dit que c'était exactement comme la confidentialité bancaire ou le fait de composer un numéro de téléphone. En appelant un numéro, tu fais l'acte volontaire de le donner à la compagnie de téléphone. Vous le saviez, pas vrai ? Quand on téléphone, au moment de composer les chiffres on dit clairement : « Je ne m'attends à aucune confidentialité. » La connexion avec la machine est encore moins explicite. Les gens ne comprennent pas comment fonctionne Internet – ils ne comprennent pas non plus comment fonctionne le téléphone –, mais les tribunaux ont systématiquement ignoré cette méconnaissance et, dans notre affaire avec Twitter, dont je ne peux malheureusement pas trop parler parce que je ne vis pas dans un pays tout à fait libre, ils pensent en gros la même chose6.

C'est totalement dingue de se dire qu'on livre toutes nos informations personnelles à ces entreprises, et que ces entreprises sont devenues pour l'essentiel une police secrète privatisée. Et – dans le cas de Facebook – on a même une surveillance démocratisée. Au lieu de payer les gens, comme le faisait la Stasi en Allemagne de l'Est, ils en tirent un bénéfice social – ils trouveront quelqu'un avec qui coucher. Ils balancent sur leurs copains, « Eh, bidule et chose se sont fiancés », « Oh, truc et machinchouette se sont séparés », « Ah, je sais qui appeler maintenant ».

ANDY : Il y a des types qui ont réussi à presser Facebook jusqu'à se faire remettre toutes les données stockées les concernant, grâce à la loi européenne sur la protection des données, et le plus petit paquet était de 350 MB, le plus gros d'environ 800 MB7. Ce qui est intéressant, c'est que la structure de Facebook a été dévoilée grâce à cette loi. Chaque fois que tu te connectes, le numéro IP et tout le reste est stocké, chaque clic que tu fais, à quelle heure, et aussi le temps que tu passes sur une page, ce qui leur permet de supposer ce que tu aimes, ce que tu n'aimes pas, etc. Et on y a découvert que l'identifiant clé de la structure de la base de données était le terme « target » (cible). Ils n'appellent pas ces gens des « abonnés » ou des « utilisateurs », ou quoi que ce soit de ce style, ils les appellent des « cibles », ce qui pourrait inviter à penser : « Tiens ! mais c'est un terme de marketing, ça. »

JULIAN : Sauf que c'est à usage interne.

ANDY : Oui, mais ce pourrait aussi être une cible au sens militaire, ou une cible au sens du renseignement. Tout dépend finalement des circonstances dans lesquelles on exploite les données.

JULIAN : OK, c'est là que ça fait vraiment peur.

ANDY : Je trouve ça très utile. On a toujours dit à propos de Facebook qu'en fait l'utilisateur n'est pas le client. L'utilisateur de Facebook est en vérité le produit, le vrai client, ce sont les boîtes de publicité. Ça, c'est l'explication la moins paranoïaque, la plus inoffensive de ce qui se trame là-bas.

Le problème, c'est qu'on peut difficilement reprocher à une entreprise de se soumettre aux lois du pays. C'est normal, et les entreprises qui ne le font pas sont hors la loi. Alors c'est un peu bizarre de dire : « Hé, ils sont en train de respecter la loi ! » C'est pas une accusation, ça.

JACOB : Non, il y a un truc que je ne peux pas laisser passer à ce sujet. Si tu fabriques un système qui enregistre tout sur quelqu'un et si tu sais que tu vis dans un pays dont les lois vont te forcer à tout balancer, alors peut-être que tu ferais bien de ne pas fabriquer ce genre de système. C'est toute la différence entre la confidentialité par la réglementation et la confidentialité par la conception quand on veut créer un système sécurisé. Quand tu cherches à cibler des individus et que tu sais que tu vis dans un pays qui cible explicitement les gens – ou si Facebook installait ses serveurs chez Kadhafi ou chez Assad –, c'est franchement négligent. Et pourtant, pas une des lettres de sécurité nationale qui ont été émises, je crois que c'était l'année dernière ou il y a deux ans, pas une ne concernait le terrorisme. Il y en a eu environ 250 000 pour tout ce qu'on voudra, mais pas pour le terrorisme8. Alors, conscientes de cette réalité, ces entreprises ont une réelle responsabilité éthique dans le fait qu'elles fabriquent ces systèmes et qu'elles ont fait le choix économique fondamental de balancer leurs clients. Et ce n'est même pas une question technique. Ça n'a rien à voir avec la technologie, ce n'est qu'une question d'économie. Elles ont considéré qu'il était plus important de collaborer avec l'État, de balancer leurs utilisateurs, de porter atteinte à leur vie privée et de participer au système de contrôle – de trouver des avantages à participer à une culture de la surveillance, de participer à une culture du contrôle – que d'y résister, alors elles s'y sont ralliées. Elles sont complices et responsables.

ANDY : Il faut dire que la responsabilité éthique n'est pas une valeur très en vogue par les temps qui courent, pas vrai ?

1. Kill your television (Tuez votre téléviseur) est le nom d'une forme de protestation contre la communication de masse qui consiste à rejeter la télévision au profit des activités sociales.

2. L'« effet de réseau » est l'effet que produit un individu accomplissant une activité sur la probabilité que d'autres accomplissent la même activité.

3. Pour plus d'information sur l'enquête du jury d'accusation, voir le chapitre « À propos des diverses tentatives de persécution de WikiLeaks et des individus qui y sont associés ».

4. Selon le Wall Street Journal, « des documents auxquels a eu accès le Wall Street Journal [montrent que] l'État américain aurait obtenu un type controversé d'ordonnance de justice secrète pour contraindre Google Inc. et le petit fournisseur d'accès Sonic.net Inc. à livrer des informations sur les comptes de messagerie électronique du membre de WikiLeaks Jacob Appelbaum... Le cas de WikiLeaks est devenu une sorte de banc d'essai de l'interprétation de la loi un peu plus tôt cette année quand Twitter a contesté une injonction intimant de remettre à la justice les archives des comptes de certains sympathisants de WikiLeaks, dont M. Appelbaum... L'ordonnance réclamait les adresses "Internet Protocol", ou IP, des appareils à partir desquels ces gens consultaient leurs comptes. Une adresse IP est un numéro unique assigné à tout appareil connecté à Internet. L'ordonnance portait aussi sur les adresses de messagerie électronique des personnes avec lesquelles communiquaient ces comptes. L'injonction a été déposée sous scellés, mais Twitter a obtenu de la cour le droit de prévenir les abonnés dont les informations étaient ainsi requises... Les ordonnances auxquelles a eu accès le Wall Street Journal réclament le même type d'informations qu'à Twitter. L'ordonnance concernant Google est datée du 4 janvier et elle enjoint le moteur de recherche géant de remettre l'adresse IP à partir de laquelle M. Appelbaum a accédé à son compte gmail.com ainsi que l'adresse email et IP des usagers avec lesquels il a communiqué depuis le 1er novembre 2009. On ne sait pas si Google a contesté l'ordonnance ou s'il a remis les documents. L'ordonnance secrète concernant Sonic est datée du 15 avril et elle enjoint Sonic de remettre le même type d'informations concernant le compte de messagerie électronique de M. Appelbaum depuis le 1er novembre 2009. Le 31 août, le tribunal a accepté de lever le secret sur l'ordonnance concernant Sonic pour en fournir une copie à M. Appelbaum ». « Secret orders target email », Wall Street Journal, 9 octobre 2011 :

http://online.wsj.com/article/SB10001424052970203476804576613284007315072.html (lien vérifié le 29 novembre 2012). Pour plus d'information, voir le chapitre « À propos des diverses tentatives de persécution de WikiLeaks et des individus qui y sont associés ».

5. « WikiLeaks demands Google and Facebook unseal US subpoenas », The Guardian, 8 janvier 2011 : http://www.guardian.co.uk/media/2011/jan/08/wikileaks-calls-google-facebook-us-subpoenas (lien vérifié le 29 novembre 2012). Pour plus de détails, voir le chapitre « À propos des diverses tentatives de persécution de WikiLeaks et des individus qui y sont associés ».

6. Voir le chapitre « À propos des diverses tentatives de persécution de WikiLeaks et des individus qui y sont associés ».

7. Pour plus de détails, voir le site Europe versus Facebook : http://www.europe-v-facebook.org/EN/Data_Pool/data_pool.html (lien vérifié le 30 novembre 2012).

8. Une lettre de sécurité nationale, National Security Letter, ou NSL, est une lettre par laquelle une agence fédérale américaine réclame des « données hors contenu » ou des « métadonnées » telles que les registres des transactions financières, les connexions IP ou les contacts mail. Quiconque reçoit

une NSL est tenu de remettre les données requises sous peine de poursuites. La NSL ne requiert pas d'autorisation de justice – elle peut être directement émise par une agence fédérale. Elle est en cela similaire à ce qu'on appelle les « injonctions administratives » (Administrative Subpoenas) – l'ordre de produire des informations qui ne requiert qu'une supervision administrative, pas judiciaire. À ce titre, les NSL pourraient constituer une violation du IVe amendement qui protège contre les perquisitions et saisies arbitraires. Les NSL comportent aussi une « clause bâillon » qui élève au rang de délit le fait qu'un individu ayant reçu une NSL en parle à qui que ce soit. À cet égard, les NSL constituent peut-être une atteinte au Ier amendement qui garantit la liberté d'expression. Dans l'affaire Doe vs Gonzales, la clause de confidentialité des NSL a été déclarée anticonstitutionnelle. La loi a été modifiée de façon à autoriser les destinataires d'une NSL à contester cette dernière devant la justice, ce qui a convaincu la cour pour le neuvième circuit que leur usage n'était plus anticonstitutionnel. Les NSL continuent de faire l'objet des critiques des associations de défense des libertés, et de recours devant les tribunaux. La pratique des NSL s'est considérablement accrue après l'approbation du Patriot Act américain en 2001. Les destinataires des NSL sont généralement des prestataires de services, comme les fournisseurs d'accès Internet ou les institutions financières. Les documents requis sont généralement ceux qui concernent les clients du destinataire. Ce dernier ne peut informer son client que ses données ont été requises. Il a le droit de contester la NSL devant la justice, mais la clause de confidentialité fait que la cible n'est même pas au courant de la NSL, ce qui le prive des moyens de se défendre devant la justice. Pour illustrer toute la difficulté de justifier une telle procédure, voir la vidéo d'une conseillère juridique du FBI qui s'efforce de répondre à la question de Jacob Appelbaum : « Comment voulez-vous que je me présente devant un juge si le tiers n'a pas le droit de me dire que je suis visé par vous ? » Sa réponse : « Il est des circonstances où nous sommes obligés de mettre ce genre de chose en place », fait froid dans le dos : http://youtu.be/dTuxoLDnmJU (qu'on retrouvera avec d'autres éléments contextuels à Privacy SOS : http://privacysos.org/node/727).

Selon l'Electronic Frontier Foundation, « De tous les pouvoirs dangereux relatifs à la surveillance par l'État qui ont été étendus par le Patriot Act, le recours à la National Security Letter (NSL) prévu par l'article 18 U.S.C § 2709 et étendu par la section 505 de PATRIOT est l'un des plus effrayants et intrusifs. Ces lettres émises à des fournisseurs de services de communication comme les compagnies de téléphone ou les fournisseurs d'accès Internet autorisent le FBI à exiger secrètement des données concernant les communications privées et l'activité sur Internet de citoyens américains ordinaires sans réelle supervision ni examen préalable de la justice. Le destinataire d'une NSL est tenu à une clause de confidentialité qui lui interdit ne serait-ce que de révéler la simple existence de cette lettre à ses collègues, ses amis, ou même à sa famille, et encore moins au public. » Voir : https://www.eff.org/issues/national-security-letters. Voir aussi les document rassemblés par l'Electronic Frontier Foundation sur les lettres de sécurité nationale rendues publiques en vertu du Freedom of Information Act : https://www.eff.org/issues/foia/07656JDB (tous les liens de cette note ont été vérifiés le 30 novembre 2012).

Combattre la surveillance totale

par les lois physiques

JÉRÉMIE : À ce stade, il est permis de se demander quelles sont les solutions disponibles, aussi bien pour un individu que pour la société dans son ensemble. Il y a d'une part des solutions techniques – la décentralisation des services, l'hébergement par chacun de ses propres données, le

cryptage, la possibilité pour l'utilisateur d'avoir une relation de confiance avec son fournisseur d'accès qui lui offre des services de cryptage, et ainsi de suite. Et puis il y a les options de réglementation dont nous avons parlé. Je ne suis pas sûr que nous soyons déjà capables de dire si l'une des deux approches est meilleure. Je pense qu'il faut développer les deux en parallèle. Il faut des logiciels gratuits que tout le monde puisse comprendre, que tout le monde puisse modifier et que tout le monde puisse examiner de près pour être bien sûr de ce qu'ils font. Je crois que les logiciels gratuits sont l'un des piliers d'une société en ligne libre, si nous voulons contrôler la machine et non être contrôlés par elle. Il faut une cryptographie puissante qui garantisse que les données que nous voulons être les seuls à pouvoir consulter ne soient lisibles par personne d'autre. Il nous faut des outils de communication comme Tor, ou comme le Cryptophone, pour ne communiquer qu'avec les interlocuteurs que nous souhaitons. Mais la puissance de l'État et de certaines entreprises sera sans doute toujours supérieure à celle des geeks que nous sommes, et à notre capacité de fabriquer et distribuer ces technologies. En mettant au point ces technologies, ces lois et ces outils pour les placer entre les mains des citoyens, peut-être faudra-t-il aussi contrôler l'usage qui est fait de la technologie – même si ce n'est pas toujours en temps réel – et sanctionner les pratiques contraires à l'éthique ou qui violent la vie privée des citoyens.

JULIAN : Je voudrais aborder ce qui m'apparaît comme une différence de point de vue entre cypherpunks américains et européens. Le IIe amendement de la Constitution américaine porte sur le droit de détenir des armes. J'ai récemment vu des images tournées par un ami aux États-Unis sur la question du droit de porter des armes, et au-dessus d'un magasin d'armes, il y avait une pancarte qui disait : « La démocratie, chargée et prête à tirer. » C'est une façon de se prémunir contre les régimes totalitaires – les gens sont armés, et le jour où ils seront vraiment à bout, ils n'auront qu'à s'emparer de leurs armes et à reprendre le pouvoir par la force. On peut se demander si cet argument demeure valable aujourd'hui, à cause de l'évolution des armes depuis trente ans. Revenons à cette affirmation selon laquelle la fabrication de codes – la diffusion de codes cryptographiques secrets que l'État ne peut pas déchiffrer – est assimilable à celle de munitions. On a fait cette grande guerre dans les années 1990 pour essayer de rendre la cryptographie accessible à tous, et on l'a largement gagnée1.

JACOB : En Occident.

JULIAN : On l'a largement gagnée en Occident, et on en voit la preuve dans tous les navigateurs, même si on assiste peut-être aujourd'hui à divers types de contournements et de détournements2. L'idée, c'est qu'on ne peut pas compter sur l'État pour mettre en place les règlements qu'il prétend mettre en place, et il faut donc fournir les outils de base, les outils cryptographiques dont nous avons la maîtrise, comme un genre de recours à la force, de sorte que si le cryptage est bon, le gouvernement aura beau tout tenter, il ne pourra pas faire intrusion dans vos communications.

JACOB : La quasi-totalité des autorités modernes tirent leur force de l'exercice ou de la menace de la violence. Il faut reconnaître à la cryptographie qu'aucune violence ne produira jamais la solution d'un problème mathématique.

JULIAN : Exactement.

JACOB : Tout est là. Ça ne veut pas dire qu'on ne pourra pas vous torturer, ça ne veut pas dire qu'ils ne pourront pas essayer de mettre votre maison sur écoute ou de la piéger d'une façon ou d'une autre, mais cela veut dire que, s'ils tombent sur un message crypté, peu importe la puissance de l'autorité qui les accompagne dans tout ce qu'ils font, ils ne pourront pas résoudre le problème mathématique. Ce fait, pourtant, n'est pas évident du tout pour les gens qui ne connaissent rien à la technique, alors il faut le divulguer. Ce serait très différent s'il était possible de résoudre tous ces problèmes mathématiques, et l'État serait évidemment capable de les résoudre lui aussi.

JULIAN : Sauf qu'il se trouve justement que c'est un fait bien réel, comme la possibilité de construire une bombe atomique : on peut créer des problèmes mathématiques qui résisteront au plus puissant des États. Je pense que ce fait a particulièrement séduit les libertaires californiens et d'autres qui croyaient à ce genre d'idée de « démocratie chargée et prête à tirer », parce que c'était une démarche très intellectuelle – une poignée d'individus maîtrisant la cryptographie et résistant à la toute-puissance du premier pouvoir mondial.

Il y a donc une propriété de l'univers qui joue en faveur de la confidentialité, puisque certains algorithmes de cryptage sont et seront toujours impossibles à décoder par quelque État que ce soit. On sait qu'il y en a d'autres qui sont très difficiles à décoder, même pour la NSA. On le sait parce qu'on recommande leur usage aux sous-traitants militaires américains pour la protection de communications ultraconfidentielles. S'ils comportaient une voie d'accès détournée, les Russes ou les Chinois ne tarderaient pas à la découvrir, et les conséquences seraient lourdes pour celui qui aurait pris l'initiative de recommander un cryptage peu sûr. Le cryptage est donc très bon aujourd'hui, il est vraiment digne de confiance. Malheureusement, on ne peut pas du tout en dire autant de la machine sur laquelle on l'utilise, et c'est à ce niveau que se situe le problème. Mais ça ne concerne pas l'interception en bloc ; ça concerne le ciblage des ordinateurs individuels. À moins d'être un spécialiste, il est en fait très difficile de vraiment sécuriser un ordinateur. Reste que la cryptographie peut quand même régler le problème de l'interception en bloc, et c'est bien ce problème-là qui menace la civilisation mondiale. La menace n'est pas dans le ciblage individuel.

Toutefois, il me semble que nous avons affaire à des forces économiques et politiques vraiment colossales, comme l'a dit Jérémie, et que l'évolution naturelle des technologies de surveillance par rapport à celle du nombre d'humains va probablement finir par lentement nous conduire vers une société totalitaire de surveillance mondiale – par totalitaire, j'entends de surveillance totale. Les derniers êtres libres seront peut-être alors ceux qui sauront utiliser cette cryptographie pour se défendre contre la surveillance absolue, totale, ainsi que certains individus totalement déconnectés, de nouveaux luddites, planqués dans des cavernes, ou des populations tribales traditionnelles qui ne possèdent aucun des outils de l'économie moderne, et n'ont donc qu'une capacité d'action extrêmement faible. On peut évidemment s'abstenir d'aller sur Internet, mais il devient alors difficile d'avoir de l'influence. Par ce choix, on se prive soi-même de toute influence. C'est comme avec les téléphones portables ; on peut choisir de ne pas en avoir, mais on réduit son influence. Ce n'est pas une façon d'avancer.

JÉRÉMIE : Si l'on considère la chose du point de vue économique, je suis persuadé qu'il existe un

marché de la confidentialité et qu'il demeure essentiellement inexploré, alors certaines entreprises vont peut-être y trouver une incitation à développer des outils qui offriront aux usagers la maîtrise individuelle de leurs données et de leurs communications. Peut-être y a-t-il là une façon de résoudre notre problème. Je ne suis pas sûr que ça puisse fonctionner tout seul, mais peut-être est-ce déjà en marche et nous ne sommes pas encore au courant.

JULIAN : La cryptographie sera bientôt omniprésente. Partout, d'importantes organisations l'utilisent, on s'oriente doucement vers des cités-États en réseau. Quand on pense aux voies de la communication sur Internet – la circulation rapide de capitaux entre pays, les organisations transnationales, les interconnexions entre les sous-parties des organisations – tout ce trafic emprunte des voies de communication qui suscitent la méfiance. C'est comme un organisme sans peau. Les organisations et les États s'interpénètrent – chaque réseau d'influence mondiale luttant pour obtenir l'avantage – et leurs flux de communications sont exposés aux opportunistes, aux concurrents, etc. De nouveaux réseaux sont donc en cours de constitution au-dessus d'Internet, des réseaux virtuels privés, et leur caractère privé est permis par la cryptographie. C'est une base industrielle puissante qui empêche qu'il y ait une interdiction de la cryptographie.

Prenons le téléphone BlackBerry, par exemple. Il possède un système de cryptage intégré qui fonctionne au sein du réseau BlackBerry. Research In Motion, l'entreprise canadienne qui le détient, peut décrypter le trafic de ses utilisateurs réguliers et possède des centres de données au Canada et au Royaume-Uni, au moins, de sorte que l'alliance anglo-américaine de partage du renseignement a accès aux communications de BlackBerry à BlackBerry dans le monde entier. Mais les grandes entreprises l'utilisent de façon plus sécurisée. Les États occidentaux n'y ont vu aucun problème jusqu'au moment où c'est sorti du cadre des entreprises pour toucher les individus – alors sont apparues les mêmes réactions politiques hostiles que dans l'Égypte de Moubarak3.

Je crois que la seule défense qui puisse efficacement nous protéger de la dystopie de surveillance annoncée sera celle où chacun prendra lui-même des mesures pour préserver son intimité, parce que ceux qui ont la capacité de tout intercepter n'ont aucune raison de s'en priver. On pourrait établir une analogie historique avec la façon dont les gens ont appris à se laver les mains. Il a fallu que la théorie microbienne de la maladie soit établie et divulguée, et qu'on insuffle la paranoïa de la propagation des maladies par l'intermédiaire de trucs qu'on a sur les mains et qui sont invisibles, comme l'est l'interception de masse. Une fois que cette connaissance a atteint un certain niveau, les fabricants de savon ont commercialisé des produits que les gens ont consommés pour apaiser leurs angoisses. Il est nécessaire d'instiller la peur chez les gens pour leur faire percevoir la situation, et cela créera une demande suffisante pour résoudre le problème.

Il y a aussi un problème de l'autre côté de l'équation, c'est que les programmes qui se prétendent sûrs, qui prétendent contenir de la cryptographie, sont souvent une arnaque, parce que la cryptographie est complexe, et que l'arnaque est dissimulable dans la complexité4.

Il faudra donc que les gens y réfléchissent. La seule question, c'est de quel côté va les porter leur réflexion. Soit ils vont penser : « Il faut que je fasse attention à ce que je dis, je dois me conformer », tout le temps, à chaque occasion. Ou alors ils vont se dire : « Il faut que j'apprenne à maîtriser les petits composants de cette technologie et que j'installe des choses qui me protègent pour que je puisse librement exprimer mes pensées et communiquer avec mes amis et ceux que j'aime. » Si les gens ne penchent pas dans ce dernier sens, alors le politiquement correct deviendra universel, parce que même lorsqu'ils communiqueront avec leurs plus proches amis, ils pratiqueront l'autocensure et renonceront à leur place d'acteurs politiques.

1. Voir plus haut la note 6 p. 216 sur les « premières guerres du cryptage » des années 1990.

2. Julian fait ici allusion au SSL/TLS, un protocole cryptographique aujourd'hui intégré d'office dans tous les navigateurs Internet et qui sert à sécuriser la navigation – par exemple quand on gère ses comptes bancaires.

3. Pour un exemple parmi beaucoup d'autres, voir « Blackberry, Twitter probed in London riots », Bloomberg, 9 août 2011 : http://www.bloomberg.com/news/2011-08-09/blackberry-messages-probed-in-u-k-rioting-as-police-say-looting-organized.html (lien vérifié le 30 novembre 2012).

4. Un membre du groupe LulzSec, qui avait mis au jour des failles dans le dispositif de sécurité de Sony en produisant les données personnelles de clients de Sony, a par exemple été arrêté quand son identité a été obtenue auprès du site proxy Hide My Ass!, par ordonnance judiciaire aux États-Unis. Voir « Lulzsec hacker pleads guilty over Sony attack », BBC, 15 octobre 2012 : http://www.bbc.com/news/technology-19949624 (lien vérifié le 30 novembre 2012).

Internet et la politique

JÉRÉMIE : Il est intéressant de constater le pouvoir que détiennent les hackers – « hackers » au premier sens du terme, pas au sens de criminel. Un hacker est un passionné de technologie, quelqu'un qui aime en comprendre le fonctionnement, ne pas être piégé, la faire mieux fonctionner, au contraire. Je suppose qu'à cinq ou sept ans, vous aviez un tournevis et vous tentiez de démonter des appareils pour voir comment c'était fait à l'intérieur. C'est ça, être un hacker, et les hackers ont créé Internet pour un tas de raisons, entre autres parce que c'était amusant, et ils l'ont développé et donné à tout le monde. Des entreprises comme Google ou Facebook ont alors vu l'opportunité de créer des modèles d'affaires fondés sur la collecte des données personnelles des utilisateurs. Mais on voit que les hackers possèdent toujours une certaine forme de pouvoir. Ce qui m'intéresse plus que tout aujourd'hui, c'est le fait que le pouvoir de ces hackers s'accroît encore, même dans l'arène politique. Aux États-Unis, il y a eu la loi SOPA (Stop Online Piracy Act – loi pour faire cesser le piratage en ligne) et la loi PIPA (Protect Intellectual Property Act – loi de protection de la propriété intellectuelle) – des lois brutales sur le copyright qui en gros donnaient à Hollywood le pouvoir d'ordonner à toute entreprise Internet de censurer et de restreindre l'accès au réseau1.

JULIAN : Et de créer des blocus bancaires comme celui que subit toujours WikiLeaks2.

JÉRÉMIE : Exactement. Ce que les banques ont fait à WikiLeaks était en train de devenir la méthode ordinaire pour combattre les vilains pirates du copyright qui ont tué Hollywood, etc. Et on a assisté à un immense tollé de la société civile sur Internet – et pas seulement aux États-Unis, ça n'aurait pas marché si les citoyens américains avaient été les seuls à s'élever contre le SOPA et le PIPA. C'est venu de gens du monde entier, et les hackers étaient au cœur de la protestation, fournissant des outils à tout le monde pour les aider à prendre part au débat public.

JULIAN : Pour les aider à organiser la campagne.

JÉRÉMIE : Je ne sais plus si c'était sur Tumblr ou sur un autre site de ce genre, tu pouvais entrer ton numéro de téléphone sur la page d'accueil et on t'appelait pour te mettre en contact avec le Congrès. Tu te retrouvais à discuter avec un interlocuteur pour lui dire : « Cette loi, c'est une connerie. »

JACOB : Internet a été utilisé pour sa propre défense.

JÉRÉMIE : Je crois que nous, hackers, avons une responsabilité à l'égard des outils que nous élaborons et que nous distribuons au reste du monde, et on est peut-être en train de voir les premiers signes de l'efficacité que peut avoir cette responsabilité si on l'exerce de façon collective. Aujourd'hui, aux États-Unis, on débat au sujet de l'ACTA (Anti-Counterfeiting Trade Agreement, accord commercial anticontrefaçon) est un traité international qui a servi de modèle au SOPA et au PIPA3. Je reviens tout juste du Parlement européen où les individus que nous sommes, les individus barbus et crasseux que nous sommes, ont pu faire prévaloir leur volonté auprès d'une commission parlementaire. Nous lui avons montré certaines règles de procédure du Parlement européen que manifestement elle découvrait et nous avons expliqué ce qu'il fallait faire, puis il y a eu ce vote, que nous avons remporté par 21 voix contre 5, marginalisant le rapporteur britannique qui s'est retrouvé seul dans son coin. C'est une très petite partie d'un petit point de procédure sur la voie d'une victoire réelle contre l'ACTA, cet accord mondial monstrueux conçu dans notre dos pour court-circuiter la démocratie. Mais il se peut que nous, citoyens, parvenions à vaincre le monstre – assez facilement, avec les outils d'Internet, les listes de distribution, les wiki, les IRC (Internet Relay Chat), etc. – et je crois qu'on est peut-être en train d'assister à la maturation d'Internet, à son entrée dans l'adolescence, où il va pouvoir servir la société au sens large pour essayer d'apporter le changement. Il me paraît extrêmement important que nous, hackers, soyons présents avec notre savoir technologique pour mettre les gens sur la voie en leur disant : « Vous devriez utiliser cette technologie qui vous laisse la maîtrise de votre confidentialité, plutôt que Facebook ou Google », et les deux actions s'articulent plutôt bien – ou en tout cas elles peuvent bien s'articuler. C'est une petite lueur d'optimisme.

JULIAN : Jacob, concernant cette radicalisation politique de la jeunesse internaute, tu viens de passer ces deux dernières années à parcourir le monde pour parler de Tor, parler aux gens qui

veulent de l'anonymat, qui veulent que leur vie privée soit à l'abri de leur propre État, et tu as dû constater ce phénomène dans de nombreux pays. Est-ce significatif ?

JACOB : Bien sûr. Ça me paraît absolument significatif. L'exemple qui me vient immédiatement à l'esprit est celui de la Tunisie. Je m'y suis rendu après la chute de Ben Ali, et on a parlé de Tor dans une classe d'informatique à l'université, où il y avait des gens très qualifiés techniquement, et une personne a levé la main pour dire : « Et les gens mal intentionnés ? » Et elle a aligné les quatre Cavaliers de l'Infocalypse – le blanchiment d'argent, les drogues, le terrorisme et la pornographie infantile. « Et les gens mal intentionnés ? » On nous ressort constamment ces quatre choses et leur spectre sert à dénigrer les technologies de préservation de la confidentialité, parce qu'il ne fait aucun doute qu'il faut vaincre ces quatre groupes d'individus. Alors j'ai demandé à la classe : « Qui d'entre vous est déjà tombé sur la page Ammar 404 ? », la page de censure affichée par le régime de Ben Ali avant et pendant la révolution pour barrer l'accès à un site. Tous les présents dans la salle, professeur inclus, ont levé la main, excepté celle qui avait posé la question. Alors, je me suis tourné vers la jeune intervenante et je lui ai dit : « Regarde les gens autour de toi. Ce sont tes camarades de classe. Tu crois vraiment que ça vaut la peine d'opprimer chacune des personnes ici présentes pour combattre ces choses-là ? », et elle a dit : « En fait, moi aussi je lève la main. »

En vérité, ça a été un peu plus laborieux, mais, dans l'ensemble, il suffit de remettre les choses dans leur contexte pour que les gens comprennent de quoi il retourne vraiment. Cela change radicalement la donne. Et ça arrive dans le monde entier, sans arrêt – mais généralement après coup, c'est- à-dire que les gens s'aperçoivent avec le recul qu'ils auraient pu utiliser la technologie : « Mais oui, ce ne sont pas seulement les gens mal intentionnés, parce qu'en fait, dès que je dis ce que je pense de quelque chose et qu'un type au pouvoir n'aime pas ce que j'ai à dire, c'est moi le mal intentionné. » Alors on voit bien qu'il y a une prise de conscience.

Mais on ne peut pas dire que ça n'arrive que depuis un an ou deux. Désolé de te faire ce coup-là, Julian, mais tu es l'une des causes de la radicalisation de ma génération. Je suis un cypherpunk de la troisième génération, si on veut compter comme ça.

Le travail que tu as accompli avec Ralf Weinmann sur le système de fichiers Rubberhose est en partie ce qui m'a donné envie de travailler sur les systèmes cryptographiques. Le système de cryptage que j'ai conçu, le MAID, est venu en réaction à des choses comme la régulation des pouvoirs d'investigation au Royaume-Uni, où l'État a décidé en gros que la régulation négative serait la solution à la cryptographie, où on peut te prendre ton mot de passe4. Évidemment, dans le cas de Julian, quand ils ont créé ça, c'était parce que des régimes d'oppression torturaient des gens pour un mot de passe, alors il fallait pouvoir livrer plusieurs mots de passe, pour obéir. Mon système de fichiers cryptographiés, le MAID, a été conçu pour un système juridique où l'accusé a le droit de garder le silence, mais où il peut prouver, si on l'y force, qu'il dit la vérité sans violer la confidentialité. J'avais compris en voyant le travail de Julian qu'on pouvait utiliser la technologie pour offrir aux gens ordinaires la capacité de changer le monde. Si on remonte très, très loin dans le temps, à la vieille liste de diffusion Cypherpunk avec Tim May, l'un de ses membres fondateurs, et si on lit les vieux posts de Julian sur la liste Cypherpunk, c'est ce qui a amené toute une génération d'individus à vraiment se radicaliser, parce que les gens ont compris qu'ils n'étaient plus atomisés, qu'ils pouvaient prendre le temps d'écrire un logiciel capable de donner du pouvoir à des millions d'individus5.

Il y a juste quelques conséquences imprévues dans la façon dont ça s'est passé, parce que les créateurs de Google n'ont pas commencé avec l'intention de créer la plus grande machine de surveillance de l'histoire. Mais, dans les faits, c'est ça qu'ils ont fait et, aussitôt qu'on s'en rend

compte, ils se mettent à envoyer ces lettres de sécurité nationale, n'est-ce pas ?

JÉRÉMIE : Je pense qu'il y a trois points essentiels dans ce que tu viens de dire.

JACOB : Seulement trois ?

JÉRÉMIE : Parmi d'autres.

ANDY : OK, permettez-moi d'en ajouter un quatrième, peut-être ?

JACOB : Tu ne connais même pas les trois autres pour l'instant.

JÉRÉMIE : Je vois trois points qui sont entrelacés. Je ne dis pas qu'il faut les prendre séparément, mais l'un d'eux concerne les régimes autoritaires et le pouvoir qu'ils détiennent à l'ère des technologies numériques. Dans le cas du régime de Ben Ali – c'est vraiment évident dans beaucoup de régimes aujourd'hui –, on peut décider de ce que les gens ont le droit de savoir ou avec qui ils vont communiquer. C'est un pouvoir considérable, il faut s'y opposer, et Internet – l'Internet libre – est un outil qui permet de le faire. Un autre point est celui de l'élaboration des outils, une meilleure technologie, une technologie capable de chercher à contourner des problèmes tels que la censure, mais fondamentalement élaborer des outils qui fassent partie de cette infrastructure qui nous aide à renverser les dictateurs. Et puis il y a la question de la fable politique que tu évoquais avec les quatre Cavaliers de l'Infocalypse, les prétextes que brandissent chaque jour les politiciens dans les médias – « Allons-nous tous mourir à cause du terrorisme ? Il nous faut un Patriot Act » ; « La pornographie infantile est partout » ; « Internet est truffé de pédo-nazis, il faut de la censure. »

JACOB : Des pédo-nazis ?

JÉRÉMIE : Oui, des pédo-nazis – le nom pedo-nazi.com est déjà réservé. « Les artistes vont mourir et le cinéma va disparaître, il faut donner à Hollywood le pouvoir de censurer Internet », et ainsi de suite. Je crois que là encore Internet est un outil, un antidote au récit politique. Le récit politique repose sur l'émotion et un temps médiatique extrêmement court – l'information apparaît et disparaît en vingt-quatre heures, puis elle fait place à une nouvelle information. Avec Internet, j'ai l'impression que nous sommes en train de créer ce que j'appelle le temps Internet. Le grand Internet n'oublie jamais rien, alors on peut constituer des dossiers pendant des années, jour après jour, et on peut élaborer, analyser. J'ai passé les trois dernières années à faire ça à propos de l'ACTA. Une fois de plus, WikiLeaks a été une source d'inspiration pour nous parce que la première version de

l'ACTA qui a fuité, ça s'est fait par WikiLeaks en 20086.

JULIAN : Oui, on l'a reçue.

JÉRÉMIE : Et on a nous-mêmes rendu publiques deux versions. Il y a eu cinq versions de ce texte en trois ans, qu'on a pu reprendre paragraphe par paragraphe, ligne par ligne, en disant là, ça veut dire ça ; là, c'est l'industrie qui réclame ça, et on a pu faire intervenir des experts juridiques et des experts technologiques pour construire une version différente de la fable politique officielle : « Oh, il nous faut l'ACTA pour sauver la culture et sauver les enfants des faux médicaments », et tout le tralala. Alors on a construit notre propre ligne politique dans le temps Internet, avec des analyses précises, beaucoup de travail, en connectant les gens pour qu'ils y participent.

JULIAN : C'est vrai, et je crois que cette perception de l'ACTA a conquis le public.

JÉRÉMIE : Jusqu'ici, ça s'est bien passé.

JULIAN : À mon avis, c'est ce que retiendra l'histoire, mais en coulisses, cette prétendue loi commerciale anticontrefaçon, dont l'industrie du copyright américaine est à l'origine, a servi concrètement dans tout un tas de traités bilatéraux à créer un nouveau régime international en matière de légalité et d'illégalité dans le domaine de la publication, et donc avait pour but d'empêcher les gens de publier un certain nombre de choses. Elle normalise une version dure du DMCA (Digital Millennium Copyright Act) américain qui prévoit que si l'on envoie une lettre à quelqu'un pour exiger qu'il retire quelque chose d'Internet, il doit commencer par le faire, puis il entre dans une espèce de procédure de deux semaines au cours desquelles il peut produire des arguments contraires et ainsi de suite. Étant donné que la gestion de cette argumentation coûte cher à n'importe quel fournisseur d'accès, il retire tout de suite l'élément incriminé puis demande à l'auteur ou à celui qui l'a mis en ligne de mener sa contestation tout seul. Ça a eu un effet assez fort aux États-Unis, où beaucoup de contenus ont été supprimés. La scientologie en a abusé pour faire retirer littéralement des milliers de vidéos de YouTube7.

Alors admettons que l'ACTA ait été mis KO au Parlement européen, que ça ait vraiment marché, en tout cas pour cette version. Les principales conséquences de l'ACTA sont malgré tout toujours là – il y a eu débat démocratique, l'ACTA a été diabolisé dans la sphère publique, on a gagné sur le plan du récit mais, en coulisses, des traités bilatéraux ont été secrètement signés qui aboutissent au même résultat, ça n'a fait que contourner le processus démocratique. Par exemple, WikiLeaks s'est procuré et a publié le nouveau traité de libre-échange entre les États-Unis et l'Inde, et on y retrouve des passages entiers de l'ACTA8. C'est aussi arrivé avec un certain nombre d'autres accords et de lois. On a peut-être réussi à décapiter l'ACTA, mais son corps va se diviser en petits bouts qui vont aller s'insinuer ici et là, dans l'ordre international que dessinent tous ces traités bilatéraux. On peut donc tenir une victoire démocratique qui a lieu en public, en surface, mais en dessous les choses se produisent quand même. Pour toutes ces raisons, je ne pense pas que la réforme de la réglementation ou de la loi soit la voie à suivre ; même si on ne peut pas non plus faire de cadeau à

l'adversaire, parce qu'il ne cherchera qu'à accélérer les choses. Il est donc important de le tenir en échec sur plusieurs fronts, comme on le fait avec l'ACTA. Ça le ralentit. Mais même une victoire au Parlement en matière de législation ne met pas fin à cette activité en sous-main.

JACOB : Il y a une chose qui mérite à mon avis d'être soulignée, c'est que Roger Dingledine, l'un des créateurs de Tor, dont je dirais qu'il est un peu mon mentor et qu'il a vraiment beaucoup guidé ma réflexion sur le contournement de la censure et l'anonymat en ligne, dit que les pare-feu, par exemple, sont non seulement une réussite technique – et il est important de comprendre la technologie qui les sous-tend si on veut construire une technologie qui y résiste –, mais une réussite sociale. Les opposants à l'ACTA utilisent la technologie, et la technologie leur permet de résister, mais ce qu'il faut vraiment considérer ici, c'est la démarche des gens ordinaires, et le jargon technique n'est pas en l'occurrence le plus important. Le plus important, c'est que les gens s'impliquent pour de bon dans ce récit et dans sa modification tant qu'ils en ont encore les moyens, et l'aspect humain est, au fond, le plus important. WikiLeaks a rendu publics des documents qui permettent d'aller dans ce sens, et le partage d'informations est sans doute important, mais les gens qui s'emparent de ces informations précieuses et qui les font circuler comptent aussi beaucoup. Parce qu'il reste au moins l'argument qu'une bonne part d'entre nous vit peut-être en démocratie, que nous sommes libres, censément gouvernés par le consensus. Alors si chacun comprend ce qui se passe et arrive à la conclusion qu'il n'est pas d'accord, il devient très difficile de continuer et de faire passer ces lois et de le faire sans le consentement de ceux qui sont gouvernés.

JÉRÉMIE : Il s'agit d'augmenter le coût politique de ces mauvaises décisions pour ceux qui les prennent, et ça, on peut le faire collectivement avec un Internet libre tant qu'on le tient entre les mains.

JACOB : Mais on pourrait aussi le faire sans Internet, parce qu'il y a eu – historiquement – des sociétés libres avant Internet, c'était juste plus coûteux en termes économiques, c'était plus laborieux à certains niveaux, et c'est en vérité ce qui donne toute son importance au mouvement peer-to-peer9.

ANDY : Le quatrième point est, à mon avis, que la dimension architecturale des systèmes décentralisés est un élément central qu'il faut aussi mettre entre les mains des gens, parce qu'on est aujourd'hui confrontés au cloud computing10.

JULIAN : Il y a Facebook, qui est complètement centralisé. Twitter est complètement centralisé. Google est complètement centralisé. Tout se trouve aux États-Unis ; tout est à la merci de celui qui contrôle la force de coercition. Exactement comme la censure qui a commencé lorsque WikiLeaks a publié Cablegate et qu'Amazon a supprimé notre site de ses serveurs11.

ANDY : Et on voit bien que le cloud computing représente une incitation économique pour les

entreprises, puisqu'il leur offre un traitement des données moins coûteux dans les centres prétendument internationaux qui sont tenus par des entreprises américaines, ce qui veut dire qu'on rapatrie les données dans la juridiction américaine, exactement comme les entreprises de paiement, etc.

JULIAN : Dans cette transition vers le cloud computing, il y a une tendance assez inquiétante. D'énormes grappes de serveurs sont réunies en un seul endroit, parce qu'il est plus efficace de standardiser le contrôle de l'environnement, de standardiser le système de paiement. C'est une technique concurrentielle parce qu'il est moins cher d'empiler les serveurs au même endroit que de les disséminer partout. L'essentiel de la communication sur Internet, à l'exception des films en streaming, se fait de serveur à serveur, alors si on installe les serveurs tout près les uns des autres, c'est moins cher. On finit par se retrouver avec ces grandes ruches de serveurs reliés entre eux. Il est logique que Google, par exemple, installe ses serveurs près des grands fournisseurs de contenu, parce que les pages sont indexées par Google pour permettre les recherches. Il y a donc aux États-Unis des bâtiments immenses qui ne contiennent rien d'autre que les serveurs de différentes entreprises. C'est là que la NSA dispose d'une partie de ses points d'interception massive. Internet pourrait exister sans cette centralisation, ce n'est pas que la technologie le rende impossible, c'est juste qu'il est plus efficace de tout centraliser. Dans la compétition économique, c'est la version centralisée qui l'emporte.

ANDY : Il est très important de comprendre le point de vue architectural – des infrastructures centralisées facilitent considérablement le contrôle central et l'abus de pouvoir. C'est comme tuer le petit commerce de proximité en centralisant la vente au détail.

JULIAN : Et en allant faire ses courses dans une grande, grande multinationale comme Safeway.

ANDY : Oui, comme ça s'est passé pour nos courses. Il est très important de conserver une approche d'infrastructure décentralisée. Quand je travaillais à l'ICANN, l'Internet Corporation for Assigned Names and Numbers, qui attribue et régule les noms de domaine sur Internet, Vint Cerf, l'inventeur d'au moins une partie du protocole TCP/IP, le protocole de communication de base d'Internet, m'a appris quelque chose. Il disait toujours : « Tu sais, il y a un bon côté avec les gouvernements, c'est qu'ils ne sont jamais singuliers, ils sont toujours pluriels. » C'est-à-dire que, même au sein des gouvernements, il y a ceux qui convoitent leur propre périmètre décentralisé de pouvoir. Au sein des gouvernements, il y a donc toujours différentes factions qui s'opposent. C'est ça en fin de compte qui nous sauvera de Big Brother, ils seront trop nombreux à vouloir être Big Brother et il y aura des disputes entre eux.

JULIAN : Je n'y crois pas, Andy. Je crois qu'il y a eu jadis des élites nationales qui se faisaient mutuellement concurrence, mais qu'aujourd'hui elles s'associent en se détachant de leurs populations respectives.

ANDY : Elles s'associent, tu as raison là-dessus – et je ne suis pas sûr que nous soyons tout à fait à l'abri –, mais il y a une chance de vraiment conserver notre identité. Il faut nous accrocher à notre propre infrastructure, c'est la leçon à retenir ici – si on veut s'opposer à l'État de surveillance, au Big Brother unique, il faut étudier de quoi il est fait, voir s'il s'agit vraiment d'une association d'États centraux qui disent : « Eh, en s'associant, on peut être encore plus gagnants. » Et il faut comprendre ce qu'est notre rôle là-dedans – notre rôle est de rester décentralisés, de posséder notre propre infrastructure, de ne pas faire confiance au cloud computing et toutes ces conneries, mais d'avoir notre truc bien à nous.

JULIAN : On risque quand même de se heurter à la domination de la technique. Étant donné qu'il est vraiment plus facile d'utiliser Twitter que de créer son propre Twitter, qu'il est vraiment plus facile d'utiliser Facebook que Diaspora ou un équivalent, que le cloud computing est vraiment moins cher, ces techniques et ces services auront le dessus12. Il ne s'agit pas de dire que nous devons lancer nos propres services locaux, parce que ces services ne seront tout simplement pas compétitifs, ils ne seront jamais utilisés que par une petite minorité. Nous devons faire mieux que dire qu'il faut un Facebook du pauvre et espérer que les gens l'utiliseront.

ANDY : Eh bien, pour reparler de l'Église catholique, nous revenons à une époque où il n'y a qu'un grand émetteur de livres, puisque Amazon est en train de chercher à prendre le contrôle de la totalité de la chaîne de distribution des livres électroniques. Il faut donc que nous préservions nos moyens d'impression et d'édition. L'objectif peut paraître légèrement présomptueux, mais nous avons vu de quoi sont capables ces entreprises quand elles, ou les agences officielles à la juridiction desquelles elles sont soumises, ne veulent pas que telle ou telle chose se produise. Et il me semble que la prochaine étape sera forcément de nous doter de nos propres fonds, de sorte que même s'ils n'apprécient pas le fait que nous soutenions des projets comme WikiLeaks ou autre, nous aurons les moyens de le faire par nous-mêmes sans compter sur une infrastructure centrale qui sera soumise à une seule juridiction.

JÉRÉMIE : Je voudrais dire que je suis d'accord avec Andy. Je pense que l'architecture est importante, et que c'est un élément central de tout ce que nous défendons. Mais c'est un message que nous avons le devoir de transmettre au public, parce que nous le comprenons, en tant que hackers, en tant que techniciens qui fabriquent Internet tous les jours et qui jouent avec. Et il y a peut-être là un moyen de conquérir les cœurs et les esprits des jeunes générations. C'est pour ça que les guerres du copyright sont à mes yeux déterminantes, parce que avec les technologies de peer-to-peer, depuis Napster en 1999, les gens ont compris – capté – qu'en partageant les fichiers entre individus...

JULIAN : ... tu deviens un délinquant.

JÉRÉMIE : Non, tu fabriques une meilleure culture.

JULIAN : Non, tu deviens un délinquant.

JÉRÉMIE : Ça, c'est ce que dit la fable, mais si tu fabriques une meilleure culture pour toi-même, tout le monde utilisera Napster13.

ANDY : L'histoire de l'humanité, l'histoire de la culture, c'est celle du copiage des idées, de leur modification et de leur traitement. Si tu appelles ça du vol, tu es comme tous les cyniques.

JÉRÉMIE : Exactement ! Exactement ! La culture est faite pour être partagée.

JULIAN : Eh bien, en Occident, depuis les années 1950, il y a une culture industrielle. Notre culture est devenue un produit industriel.

JÉRÉMIE : On est en train de nourrir le troll, là, parce qu'il se fait l'avocat du diable et qu'il le fait très bien.

JACOB : Je ne marche pas. C'est évident que c'est des conneries.

JÉRÉMIE : Des conneries. Dans le récit politique, on appelle ça du vol, mais je voudrais pousser mon raisonnement au bout pour dire que tous ceux qui ont utilisé Napster en 1999 sont devenus des amateurs de musique, ils ont été aux concerts, puis ils sont devenus des prescripteurs qui disaient : « Tu devrais écouter ça, tu devrais aller à tel ou tel concert », et ainsi de suite. Ces gens ont donc vu un exemple concret de la façon dont la technologie peer-to-peer décentralisait l'architecture. En vérité, Napster était alors un peu centralisé, mais il a planté la graine de l'idée d'architecture décentralisée. Il a mis à la disposition de tous un exemple concret d'architecture décentralisée bénéfique à la société, et quand on parle de partage de culture, c'est exactement comme le partage du savoir. C'est de partage du savoir que nous parlons quand on dit qu'il faut contourner la censure, ou outrepasser le récit politique pour bâtir un système démocratique meilleur et améliorer la société.

On a donc des cas où la décentralisation du service et le partage entre individus rend les choses meilleures, et le contre-exemple nous est fourni par l'avocat du diable qu'interprète Julian, c'est quand un secteur arrive et dit : « Oh, ça c'est du vol, ça tue tout le monde, ça tue les acteurs, ça tue Hollywood, ça tue le cinéma, ça tue plein de gentils chatons, ça tue tout. » Ils ont remporté des batailles dans le passé, mais nous sommes peut-être à présent en train de remporter celle de l'ACTA. Et là encore, je ne peux que désapprouver l'avocat du diable qu'interprétait Julian tout à l'heure. L'ACTA a été le plus grand exemple de contournement de la démocratie à ce jour, de bras

d'honneur aux Parlements et aux institutions internationales, de bras d'honneur à l'opinion publique et d'imposition de mesures inacceptables par une porte dérobée. Si nous arrivons à nous en débarrasser, nous aurons créé un précédent, et cela nous donnera l'occasion de promouvoir un programme positif, de dire : « L'ACTA, c'est fini, employons-nous maintenant à faire quelque chose qui soit vraiment pour le public. » On travaille dans ce sens, et certains membres du Parlement européen comprennent à présent que lorsque des individus partagent des choses, quand ils partagent des fichiers sans faire de profit, ils ne doivent pas aller en prison, il ne faut pas les punir. Je crois que si on arrive à ça, on aura de solides arguments pour dire au reste du monde que le partage décentralisé du savoir et de l'information rend les choses meilleures, qu'il faut l'encourager et pas le combattre, et que toute tentative de s'y opposer – qu'elle vienne de la loi, d'un dictateur ou d'une entreprise – doit être combattue, point final. Je crois que nous sommes arrivés au moment où ce message peut trouver un large écho.

JULIAN : Que dire du débat PIPA/SOPA aux États-Unis ? Ce sont de nouvelles lois soumises au Congrès américain visant à créer des embargos financiers et des blocus sur Internet au nom des entreprises américaines.

JACOB : Elles ont été créées spécifiquement pour attaquer WikiLeaks et tout ce qui peut y être lié ou y ressembler.

JULIAN : Au Congrès, on a spécifiquement évoqué le blocus bancaire contre nous comme un outil efficace14.

JÉRÉMIE : Et il s'agissait de mettre cet outil entre les mains d'Hollywood.

JULIAN : Alors on a mené une grande campagne contre, et Google, Wikipédia et un tas d'autres ont fini par s'y rallier. Mais je n'ai pas pensé : « OK, génial, on a gagné la bataille. » Ça m'a surtout fichu la trouille, parce que d'un coup Google se considérait comme un acteur politique, pas comme un simple distributeur, et on a senti ce pouvoir énorme, colossal, sur le Congrès.

JÉRÉMIE : Google n'a été qu'un petit fragment de la coalition anti-SOPA et PIPA.

JACOB : Oui, et attends, il me semble que Tumblr a eu plus d'influence que Google.

ANDY : Tumblr comme Wikipédia et des tonnes d'actions individuelles, de très petites actions dont tu n'as peut-être jamais entendu parler, ont produit un effet. Il y en avait des milliers qui ont avancé

ensemble – dans la même direction – et ça, encore une fois, c'est de l'action politique décentralisée. C'est à un mouvement politique décentralisé qu'on a assisté. Google était juste le plus gros acteur que vous avez remarqué, parmi tous les autres.

JULIAN : En tout cas, c'est celui que le Congrès a déclaré avoir remarqué.

JACOB : J'ai un petit problème avec ce qu'a dit Jérémie tout à l'heure, parce que, au fond, tu défends l'idée d'une avant-garde politique. Je ne pense pas que tu l'aies fait volontairement, mais tu l'as fait quand même, alors il faut que je t'arrête tout de suite parce que le mouvement peer-to-peer est explicitement opposé à une avant-garde politique. C'est l'idée que nous sommes tous égaux et que nous pouvons partager ; on peut apporter des services différents ou on peut apporter des fonctionnalités différentes. Ross Anderson m'a dit un jour : « Quand j'ai rallié le mouvement peer-to-peer il y a cinquante ans », et j'ai trouvé que c'était une entrée en matière fantastique. Il a expliqué qu'il voulait s'assurer que nous ne désinventerions jamais la presse d'imprimerie. Parce que dès qu'on se met à centraliser les services, à centraliser les systèmes de contrôle de l'information, on se met à désinventer l'imprimerie au sens où l'encyclopédie Britannica ne produit plus des livres imprimés mais seulement des CD – si tu ne possèdes pas un ordinateur généraliste capable de lire ces CD tu n'as pas accès à ce savoir. Bon, dans le cas de l'encyclopédie Britannica ce n'est pas grave parce qu'on a Wikipédia et tout un tas d'équivalents. Mais, en tant que société, je ne crois pas que nous soyons prêts.

ANDY : Je ne suis pas sûr que Wikipédia soit si formidable que ça en tant qu'outil de référence. Je ne fais confiance à aucune des pages que je n'ai pas réécrites moi-même.

JACOB : Mais l'encyclopédie Britannica, c'est pareil. C'est juste une référence parmi tant d'autres, et ce qui compte, c'est la vérification des données. Tout ce que je veux dire, c'est qu'il ne faut pas promouvoir cette idée d'avant-garde, parce qu'elle est très dangereuse.

JULIAN : Attends un peu, pourquoi ? Je ne suis pas contre les avant-gardes. Quel est le problème ?

JÉRÉMIE : Je ne parle pas des avant-gardes, je dis simplement que nous avons de nouveaux outils entre les mains. On a évoqué l'imprimerie. Un autre visionnaire, un de mes amis, Benjamin Bayart, qui n'est peut-être pas très connu hors du monde francophone, a dit : « L'imprimerie a permis au peuple de lire, Internet va lui permettre d'écrire15. » C'est très nouveau, c'est la possibilité nouvelle pour chacun d'écrire et de s'exprimer.

ANDY : Oui, mais le filtrage est devenu encore plus important ces derniers temps.

JÉRÉMIE : Sans doute parce que tout le monde prend la parole, et que beaucoup disent des conneries. Comme l'a dit le professeur d'université et activiste Larry Lessig et comme diraient, je crois, beaucoup d'autres profs, on apprend aux gens à écrire, mais quand les étudiants remettent leur devoir, quatre-vingt-dix-neuf virgule quelque chose pour cent ne valent rien, mais cela ne nous empêche pas de leur apprenndre à écrire16. Alors, évidemment, il se dit beaucoup de conneries sur Internet – aucun doute là-dessus. Mais, à force de prendre la parole en public, avec le temps on améliore sa façon de s'exprimer, on devient de plus en plus capable de participer à des débats complexes. Et tous les phénomènes que nous décrivons s'articulent autour d'une complexité qu'il faut découper en petits morceaux pour pouvoir la comprendre et en débattre calmement. Ce n'est pas une question d'avant-garde politique, il s'agit de véhiculer à l'intérieur du système politique cette nouvelle possibilité d'expression que nous avons entre les mains, d'échanger nos idées, de participer au partage du savoir sans être membre d'un parti politique, d'un média ou de n'importe quelle autre structure centralisée qui était autrefois indispensable à celui qui voulait s'exprimer.

1. Le SOPA (Stop Online Piracy Act) et le PIPA (Protect Intellectual Property Act) sont des propositions de loi américaines qui ont beaucoup fait parler d'elles au début de l'année 2012. L'une et l'autre sont l'expression limpide du désir de l'industrie des contenus, représentée par des organismes tels que la Recording Industry Association of America, de renforcer les lois de la propriété intellectuelle à l'échelon mondial, et aussi lourdement que possible, en réponse à la libre distribution de biens culturels en ligne. Les deux textes proposaient d'accorder aux agences américaines de maintien de l'ordre un pouvoir de censure aussi exorbitant qu'étendu, qui menaçait de « casser Internet ». Les deux textes ont suscité la colère d'une bonne partie de la communauté internationale des internautes et provoqué une vive réaction des acteurs industriels qui ont intérêt à ce qu'Internet demeure libre et ouvert.

Début 2012, Reddit, Wikipédia et quelques milliers d'autres sites ont temporairement interrompu leurs services en signe de protestation, suscitant une lourde pression publique sur les élus. D'autres prestataires de services en ligne, comme Google, ont appelé à l'envoi de pétitions. Les deux lois ont donc été suspendues, en l'attente d'un réexamen et d'un débat autour de la question de savoir s'il s'agit bien de la meilleure façon d'aborder le problème de la propriété intellectuelle en ligne. L'épisode est perçu comme le premier signe d'une réelle capacité de pression de l'industrie Internet sur le Congrès américain.

2. Voir le chapitre « À propos des diverses tentatives de persécution de WikiLeaks et des individus qui y sont associés ».

3. L'ACTA, accord commercial anticontrefaçon, est un traité international multilatéral négocié en secret pendant plusieurs années à l'initiative des États-Unis et du Japon, dont une partie institue de nouvelles obligations draconiennes pour protéger la propriété intellectuelle.

Les premiers brouillons du texte ont été révélés au public en 2008 par une fuite WikiLeaks, provoquant de très vastes mouvements de protestation parmi les activistes de la culture libre et les

défenseurs d'Internet. Voir les pages consacrées à l'ACTA sur WikiLeaks : http://wikileaks.org/wiki/Category :ACTA.

Les câbles diplomatiques partagés par WikiLeaks avec La Quatrature du Net début 2011 montrent que les négociations de l'ACTA ont été volontairement tenues secrètes pour précipiter la création de règles extrêmes de protection de la propriété intellectuelle, qui seraient ensuite imposées par la contrainte aux pays pauvres exclus de l'accord. Voir « WikiLeaks Cables Shine Light on ACTA History », La Quadrature du Net, 3 février 2011 : http://www.laquadrature.net/en/wikileaks-cables-shine-light-on- acta-history (lien vérifié le 1er décembre 2012). En juillet 2012, à la suite d'une campagne menée par La Quadrature du Net et Jérémie Zimmermann, l'ACTA a été rejeté au Parlement européen.

4. Le MAID (Mutually), Assured Information Destruction [destruction d'information (mutuellement) assurée], est « un système qui détruit automatiquement les clés cryptographiques dès qu'un délai donné, configurable par l'utilisateur, a été franchi » : https://www.noisebridge.net/wiki/M.A.I.D.

Avec des lois telles que le Regulation of Investigatory Powers Act (loi de réglementation des pouvoirs d'investigation) de 2000, ou RIPA, le Royaume-Uni est un régime plutôt hostile à la cryptographie. En vertu du RIPA, tout individu peut être contraint de décrypter des données ou de remettre un mot de passe sur injonction d'un agent de police. Aucune supervision judiciaire n'est requise. Le refus d'obtempérer peut donner lieu à des poursuites pénales. Dans le procès qui s'ensuit, si l'accusé prétend avoir oublié le mot de passe, la charge de la preuve est inversée, et c'est à l'accusé de prouver qu'il a oublié le mot de passe pour échapper à la condamnation. Selon les dénonciateurs de la loi, il s'agit d'une présomption de culpabilité de fait. Par comparaison, si les mêmes questions ont suscité beaucoup de litiges aux États-Unis, et si la situation est loin d'y être idéale, l'invocation du Ier et du IVe amendement dans des circonstances similaires s'est avérée beaucoup plus efficace. Voir l'article « Freedom from Suspicion, Surveillance Reform for a Digital Age », JUSTICE, 4 novembre 2011 : http://www.justice.org.uk/resources.php/305/freedom-from-suspicion.

Pour en savoir plus à propos du système de fichiers Rubberhose, voir « The Idiot Savants' Guide to Rubberhose », Suelette Dreyfus : http://marutukku.org/current/src/doc/maruguide/t1.html (tous les liens de cette note ont été vérifiés le 1er décembre 2012).

5. On peut télécharger les archives de l'ancienne liste de diffusion Cypherpunk : http://cryptome.org/cpunks/cpunks-92-98.zip. Tim May a été l'un des fondateurs de la liste de diffusion des Cypherpunks. Voir son cyphernomicon, et une foire aux questions sur l'histoire et la philosophie cypherpunks : http://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html (liens vérifiés le 1er décembre 2012).

6. « Proposed US ACTA plurilateral intellectual property trade agreement (2007) », WikiLeaks, 22 mai 2008 : http://wikileaks.org/wiki/Proposed_US_ACTA_plurilateral_intellectual_property_trade_agreement_%282007%29 (lien vérifié le 1er décembre 2012).

7. « Massive Takedown of Anti-Scientology Videos on YouTube », Electronic Frontier Foundation, 5 septembre 2008 : https://www.eff.org/deeplinks/2008/09/massive-takedown-anti-scientology-videos-youtube (lien vérifié le 1er décembre 2012).

8. « EU-India Free Trade Agreement draft, 24 Feb 2009 », WikiLeaks, 23 juin 2009 : http://wikileaks. org/wiki/EU-India_Free_Trade_Agreement_draft,_24_Feb_ 2009 (lien vérifié le 1er décembre 2012).

9. Peer-to-peer ou P2P désigne un réseau où chaque ordinateur peut agir comme client ou comme serveur pour tous les autres (chaque ordinateur peut aussi bien donner que recevoir de l'information), ce qui permet le partage rapide de contenus tels que la musique, les vidéos, les documents ou tout type d'information numérique.

10. Le cloud computing (informatique en nuage) désigne la situation dans laquelle une part importante des fonctions habituellement accomplies par un ordinateur, comme le stockage de données (y compris les données utilisateur pour plusieurs applications), l'hébergement et l'utilisation de logiciels, ainsi que l'apport de la puissance de traitement nécessaire à l'utilisation des logiciels, s'effectue à distance, hors de l'ordinateur proprement dit, « dans le nuage » – généralement par des entreprises qui offrent leurs services sur Internet. Au lieu de l'ordinateur complet, l'utilisateur n'a plus besoin que d'un appareil capable d'accéder à Internet, le reste lui est servi à travers sa connexion. La métaphore « dans le nuage » occulte le fait que toutes les données et les métadonnées de l'utilisateur sont en vérité stockées sur un ordinateur extérieur, quelque part dans un centre de données, très probablement contrôlé par une grosse entreprise de type Amazon, et que si ce n'est plus l'utilisateur qui en détient le contrôle complet, c'est quelqu'un d'autre.

11. Voir le chapitre « À propos des diverses tentatives de persécution de WikiLeaks et des individus qui y sont associés ».

12. Diaspora est un réseau social qui permet à chaque utilisateur de devenir son propre serveur en installant le logiciel Diaspora, grâce auquel il garde le contrôle de ses propres données. Il a été créé pour fournir une alternative respectueuse de la vie privée à Facebook. Il est à but non lucratif et appartient à ses utilisateurs : http://diasporaproject.org.

13. Le Napster des origines (1999-2001) était un service pionnier de partage de musique peer-to-peer. À cause de son immense succès, il a été rapidement fermé à la suite d'un recours en justice déposé par la Recording Industry Association of America pour infraction à la propriété intellectuelle. Après sa faillite, Napster a été racheté et transformé en boutique de vente de musique en ligne.

14. Voir le chapitre « À propos des diverses tentatives de persécution de WikiLeaks et des individus qui y sont associés ».

15. Benjamin Bayart est le président de French Data Network, le plus ancien fournisseur d'accès à Internet en France encore en activité, qui défend la neutralité d'Internet et les logiciels libres. Voir sa fiche Wikipédia : http://fr.wikipédia.org/wiki/Benjamin_Bayart (lien vérifié le 2 décembre 2012).

16. Larry Lessig est un professeur d'université et activiste américain surtout connu pour ses opinions sur le droit d'auteur et la culture libre. Il tient un blog : http://lessig.tumblr.com (lien vérifié le 2 décembre 2012).

Internet et l'économie

JULIAN : J'aimerais qu'on parle de trois libertés fondamentales. Quand j'ai interviewé le chef du Hezbollah, Hassan Nasrallah...

JACOB : Alors, ça vient cette putain d'attaque de drone ? C'est quoi, ce bruit là-haut ?

JULIAN : En fait, lui aussi est aux arrêts domiciliaires, en quelque sorte : il doit se cacher dans un endroit tenu secret et ne peut pas mettre le nez dehors.

JACOB : Cette comparaison me met mal à l'aise. Je préférerais qu'on l'évite...

JULIAN : On peut se poser la question : le Hezbollah dispose-t-il des attributs d'un État ? Est-il, en fait, devenu un État ? Le Hezbollah a mis en place son propre réseau de fibre optique au Sud-Liban, c'est dit dans les télégrammes de l'ambassade américaine1. Il dispose donc des trois principaux attributs qui font un État : le monopole de la force armée sur une région, le contrôle de l'infrastructure de communication et le contrôle de l'infrastructure financière. On peut aussi envisager ces trois éléments du point de vue de trois libertés fondamentales.

La liberté de mouvement – la liberté physique d'aller et venir, la capacité de se déplacer sans que l'on vous oppose la force armée.

La liberté de pensée – et la liberté de communiquer qui va de pair, parce que si l'on vous menace en raison de vos opinions, la seule manière de préserver votre droit de communiquer, c'est de communiquer de manière privée.

Et enfin la liberté d'interagir économiquement. Parlons donc de l'idée que les cypherpunks ont développée à partir des années 1990, à savoir qu'il fallait défendre cette troisième liberté essentielle, la liberté d'interaction économique.

JÉRÉMIE : Pourquoi se limiter à trois libertés fondamentales ? Dans la Charte des droits fondamentaux de l'Union européenne, elles sont bien plus nombreuses.

JULIAN : La confidentialité est également importante puisque, du point de vue de la communauté, il ne peut y avoir de liberté de pensée et de communication sans elle ; et elle l'est également du point de vue économique puisqu'il ne peut y avoir de liberté d'interaction sans elle. Donc oui, j'estime qu'il existe d'autres libertés, dérivées, mais que celles-ci – les trois que je viens de citer – sont celles dont découlent les autres.

JÉRÉMIE : Il existe une définition légale des libertés fondamentales.

JULIAN : J'ai lu la Charte des droits fondamentaux de l'Union européenne, et je peux vous dire que c'est un vrai foutoir consensuel.

JÉRÉMIE : Oui, d'accord, il est vrai que les lobbies ont réussi à y inscrire la propriété intellectuelle.

JULIAN : Et toutes sortes de trucs complètement déments.

ANDY : Je crois que nous sommes d'accord sur au moins un point, à savoir que le système monétaire actuel, l'infrastructure économique permettant d'échanger des sommes d'argent, craint vraiment. Je pense que, même si vous ne possédez qu'un simple compte sur eBay, vous serez d'accord là-dessus : ce que fait PayPal, ce que font Visa et MasterCard, c'est soumettre les gens à un monopole de fait. Dans les télégrammes du Cablegate, il y avait quelque part une information très intéressante : le gouvernement russe avait essayé d'obtenir que les paiements Visa et MasterCard effectués par des citoyens russes sur le territoire russe soient traités en Russie même. Visa et MasterCard ont dit non2.

JULIAN : Eh oui, l'ambassade américaine et Visa ont assez de pouvoir pour empêcher un État, et pas n'importe lequel, la Russie, de disposer de son propre système de paiement par carte de crédit.

ANDY : Ça veut dire que même les paiements effectués par des citoyens russes dans des magasins russes sont traités par des data centers américains. Et seront donc sous la juridiction du gouvernement américain, qui peut, au bas mot, être au courant de tout ce qui se passe là-bas.

JULIAN : Quand Poutine sort acheter un Coca, Washington est au courant trente secondes plus tard.

ANDY : C'est une situation intolérable, bien évidemment, quoi que l'on pense des États-Unis. Il est tout bonnement dangereux que les paiements soient tous enregistrés au même endroit, ces données se prêteront forcément à des exploitations de toutes sortes.

JACOB : Une des choses fondamentales qu'avaient comprise les cypherpunks, c'est que l'architecture définit la politique – si ton architecture est centralisée, et même si ceux qui la contrôlent sont totalement irréprochables, elle attirera des enfoirés et ces enfoirés se serviront de leur pouvoir pour faire ce que les premiers concepteurs ne se seraient jamais permis. Et il faut bien comprendre que pour l'argent, c'est pareil.

JULIAN : C'est comme les puits de pétrole en Arabie saoudite, la malédiction du pétrole.

JACOB : La règle générale, dans tous les domaines et en particulier dans le domaine financier, c'est que les meilleures intentions du monde ne valent rien. La vérité, c'est l'architecture. Pour les télécommunications, il suffit de regarder Internet. Les systèmes d'interception prétendument légalisés, ce n'est qu'un euphémisme pour cacher le fait qu'on espionne les gens...

JULIAN : C'est de la langue de bois, l'interception légalisée.

JACOB : Absolument, comme les assassinats légalisés.

ANDY : Ou la torture légalisée.

JACOB : Vous savez que Barack Obama a autorisé des attaques de drones contre des citoyens américains ? Il a fait tuer le fils d'Anwar al-Awlaqi, âgé de seize ans, au Yémen, et c'était un meurtre légal, un assassinat ciblé, comme ils disent3. Les interceptions prétendument légales, c'est pareil – on accole « légal » à n'importe quoi et tout d'un coup, parce que c'est un État qui fait ça, c'est légitime. Mais, en fait, la seule chose qui leur permette de te faire ça, c'est l'architecture de l'État, l'architecture des lois, et l'architecture de la technologie, et il en va de même pour l'architecture des systèmes financiers.

Les cypherpunks voulaient créer des systèmes qui permettraient vraiment d'effectuer des transactions en toute liberté, sans que personne ne puisse interférer, sur le modèle des monnaies chaumiennes – des monnaies électroniques conçues conformément aux spécifications de David Chaum, l'inventeur d'eCash (une monnaie électronique totalement anonyme) dont je sais que vous allez me dire qu'elles étaient encore trop centralisées. L'idée est de trouver la façon de créer des monnaies anonymes, à l'opposé de ce que font Visa et MasterCard qui ont mis en place des systèmes permettant de vous suivre à la trace. Même si elles sont bâties autour d'une autorité centrale, les monnaies chaumiennes utilisent des protocoles cryptographiques inventés par David Chaum qui garantissent l'anonymat des transactions4.

JULIAN : De l'argent électronique sans numéros de série.

JACOB : Ou avec des numéros de série permettant juste de vérifier qu'il s'agit d'argent en bonne et due forme, mais pas de savoir qui a payé qui, ni même quelle somme a été échangée.

JÉRÉMIE : En fait, cela revient à réinventer les espèces dans le monde numérique.

JULIAN : La mise au point de monnaies électroniques est essentielle parce que le contrôle des moyens d'échange est l'un des trois attributs d'un État, comme je le disais à propos du Hezbollah. Si tu prives l'État du monopole sur les moyens d'interaction économique, tu lui retires l'un de ses trois principaux ingrédients. Dans le modèle de l'État-mafia, où l'État est un racket de protection, celui-ci extorque de l'argent aux gens par tous les moyens imaginables. Le contrôle des flux monétaires est important pour que l'État puisse s'assurer des revenus, mais il lui permet également de contrôler les activités des gens – favoriser ou inhiber telle ou telle activité, interdire certaines activités ou organisations, ou certaines interactions entre organisations. Donc, par exemple, si l'on considère l'incroyable blocus financier décrété contre WikiLeaks, ce n'est pas le libre marché qui a décidé de l'imposer, parce qu'il ne s'agit pas d'un libre marché – la réglementation gouvernementale donne un pouvoir exorbitant à certains acteurs financiers et interdit à d'autres d'accéder librement au marché. La liberté économique est sous la coupe d'une élite qui influe à la fois sur la régulation et sur les principes de fonctionnement des banques5.

ANDY : C'est triste à dire, mais il s'agit du principal problème du monde électronique en ce moment. Deux compagnies de crédit, disposant chacune d'une infrastructure de compensation électronique basée aux États-Unis – ce qui place leurs données sous juridiction américaine –,

contrôlent la plus grande partie des paiements par carte de crédit dans le monde. Une compagnie comme PayPal, qui est aussi soumise à la législation américaine, applique des politiques américaines, par exemple en interdisant à des marchands en ligne allemands de vendre des cigares cubains, ou en imposant un blocus à WikiLeaks dans des juridictions non américaines. Le gouvernement américain a accès aux données et peut contrôler des paiements à l'échelle planétaire. Les citoyens américains estiment peut-être que leur démocratie est la meilleure que l'on puisse trouver sur le marché, mais, pour les citoyens européens, le prix est inacceptable.

JULIAN : Dans le monde traditionnel, il existait une liberté de déplacement, même si elle n'était pas totale.

JACOB : Tu en es sûr ? Ta liberté de déplacement actuelle est un exemple classique de la réalité de cette liberté-là.

JULIAN : Oui, bien sûr. Le Royaume-Uni vient d'annoncer qu'il compte placer 100 000 personnes par an dans ma situation6. Pas sûr qu'on puisse parler de dommages collatéraux...

JACOB : C'est la raison pour laquelle les fondateurs de mon pays fusillaient les Anglais. Il y avait une bonne raison à cela, et elle est toujours là ! La tyrannie est une réalité.

JÉRÉMIE : Pas d'attaques personnelles, s'il vous plaît.

ANDY : En attendant, ton pays, les États-Unis, privatise des prisons en négociant des contrats qui garantissent aux concessionnaires un taux de remplissage de 90 %7. C'est quoi, ça ? L'absurdité du capitalisme poussée à son comble.

JULIAN : Il y a plus de gens en prison aujourd'hui aux États-Unis qu'il n'y en avait en Union soviétique.

JACOB : Tout ça, c'est l'argument fallacieux selon lequel je devrais m'abstenir de contester quelque chose qui est mauvais sous prétexte que je fais partie de quelque chose qui l'est tout autant. Je ne pense pas que les États-Unis soient un exemple de perfection. Mais je pense qu'il y a plein de très bonnes choses aux États-Unis, comme la rhétorique des Pères fondateurs.

JULIAN : Ces dix dernières années, la rhétorique des Pères fondateurs a pris un sacré coup.

JACOB : N'oublions pas que ce qu'on raconte sur la rhétorique des Pères fondateurs relève souvent du mythe et qu'il faut se garder de les idéaliser. Donc, je suis évidemment d'accord. Tout ce que je voulais dire par ma remarque sur la tyrannie britannique et la situation dans laquelle se trouve Julian, c'est que cela est culturel. C'est là que la société entre en jeu et joue un rôle très important, et la technologie peut difficilement s'y substituer. Les questions financières sont parmi les plus dangereuses auxquelles on puisse s'intéresser. Ce n'est pas pour rien que le créateur d'une autre monnaie électronique, Bitcoin, préfère rester anonyme. Tu ne veux pas être celui qui aura inventé la première monnaie électronique vraiment opérationnelle8.

JULIAN : Les types qui ont inventé e-gold ont fait l'objet de poursuites aux États-Unis9.

JACOB : C'est vraiment hyperénervant.

JULIAN : J'aimerais revenir à la question des trois libertés fondamentales. La liberté de communiquer, la liberté de circuler, la liberté d'interagir économiquement. Lorsque notre société globale a fait sa transition vers Internet, lorsque cette transition a eu lieu, la liberté de circuler n'a pas été essentiellement modifiée. La liberté de communiquer a été incroyablement amplifiée à certains égards, dans la mesure où aujourd'hui on a les moyens de communiquer avec un nombre bien plus important de personnes ; mais, d'un autre côté, cette liberté s'est gravement détériorée, parce que le respect de la vie privée a été battu en brèche. Il est devenu possible d'espionner toutes nos communications et on ne se prive pas de le faire, et toutes ces données sont conservées et pourront ensuite être utilisées contre nous. L'interaction élémentaire que nous avons avec des personnes physiques s'est donc détériorée.

ANDY : On peut protéger sa vie privée, mais cela a un coût.

JULIAN : Nos interactions économiques ont subi les mêmes effets. Autrefois, dans une interaction économique traditionnelle, qui était au courant ? Les personnes qui vous avaient vu vous rendre au marché. Aujourd'hui, qui est au courant ? Si vous achetez quelque chose à votre voisin en vous servant de votre carte Visa – ce que vous auriez pu faire de manière presque entièrement anonyme dans une société de marché traditionnelle –, qui sera au courant ?

JACOB : Tout le monde.

JULIAN : Tout le monde. Les puissances occidentales partagent toutes leurs données, elles sont au courant, et elles enregistrent tout ça quelque part, pour toujours.

ANDY : Julian, ce que tu dis n'est pas faux, mais je me demande si l'on peut vraiment distinguer la liberté de communiquer de la liberté d'interagir économiquement, parce que Internet tel qu'il existe aujourd'hui sert d'infrastructure à toutes nos interactions, qu'elles soient économiques, culturelles ou politiques.

JACOB : On peut certainement les distinguer de la liberté de mouvement.

ANDY : Quelle que soit l'architecture de communication, l'argent c'est simplement des bits. C'est juste une utilisation d'Internet. Si le système économique repose sur l'infrastructure électronique, l'architecture de l'infrastructure électronique dit quelque chose sur la manière dont l'argent circule, est contrôlé, centralisé et ainsi de suite. Internet n'a pas été conçu pour servir d'infrastructure, mais la logique économique s'est imposée : « C'est moins cher de faire ça avec Internet. » Les banques et les sociétés de cartes de crédit avaient des distributeurs de billets avec des interfaces X.25, qui constituaient un réseau indépendant il y a dix ou vingt ans. De nos jours, tout est TCP/IP parce que c'est moins cher10. L'architecture de la technologie est en train de devenir une question essentielle parce qu'elle détermine tous les autres domaines, voilà ce qu'il faut repenser. Si nous souhaitons un moyen décentralisé de gérer nos paiements, nous devons prendre l'infrastructure en main.

JACOB : Bitcoin possède pas mal de caractéristiques souhaitables pour une monnaie électronique.

ANDY : Et elle ne génère pas d'inflation.

JACOB : Bitcoin fonctionne de manière décentralisée, donc au lieu d'avoir la réserve fédérale, tu as tout un tas de gens à travers le monde qui se mettent d'accord pour définir la réalité des transactions, et de la monnaie qu'ils utilisent.

JULIAN : Et tout cela est rendu possible par des logiciels.

JACOB : J'aimerais expliquer cela en des termes non techniques. Bitcoin est une monnaie électronique qui ressemble davantage à une marchandise échangeable qu'à de l'argent, dans la mesure où ce sont les utilisateurs qui décident combien d'euros vaut un bitcoin. Dans ce sens, cela ressemble un peu à l'or, d'ailleurs on parle du « coût d'extraction » d'un bitcoin, quand ton ordinateur fait une recherche pour trouver un bitcoin. L'idée est que la complexité computationnelle

de ce travail d'extraction détermine la valeur de la chose. Pour parler comme tout le monde, cela me permet d'envoyer de l'argent à Julian et à Julian de me confirmer qu'il l'a bien reçu sans qu'Andy ni qui que ce soit d'autre puisse intervenir ou s'y opposer. Cela dit, tout n'est pas parfait dans Bitcoin, l'anonymat n'est pas respecté, ce qui à mon sens est un problème.

JULIAN : Bitcoin est un hybride très intéressant : les titulaires des comptes sont privés et chacun peut ouvrir un compte quand bon lui semble, mais les transactions sont entièrement publiques. C'est le principe même de son fonctionnement, et on ne peut pas faire autrement si l'on veut que les gens puissent tomber d'accord sur la réalité d'une transaction : il faut pouvoir vérifier que le compte émetteur a été débité d'un certain montant et que le compte destinataire a été crédité exactement du même montant. C'est une des manières de faire marcher un système monétaire décentralisé, sans serveur central, qui pourrait être la cible d'une tentative de contrôle forcé. Dans Bitcoin, c'est la distribution qui est vraiment innovante, ainsi que les algorithmes qui permettent cette distribution, aucune partie du système bancaire Bitcoin n'étant plus digne de confiance qu'une autre, en quelque sorte. La confiance, en fait, est distribuée. Et la régulation ne se fait pas par l'intermédiaire de lois, de règlements ou d'audits, mais en tenant compte de la complexité du calcul cryptographique que doit effectuer chaque partie du réseau pour démontrer qu'elle fait bien ce qu'elle dit. Donc, l'honnêteté du « système bancaire » Bitcoin est inscrite dans son architecture même. La complexité du calcul est reflétée par des coûts en électricité pour chaque banque Bitcoin, et on peut donc calculer le coût de la fraude en fonction des coûts électriques. Le travail requis pour frauder suppose des coûts électriques plus élevés que le bénéfice économique escompté. C'est très innovant, moins au niveau des idées (qui circulent sur le papier depuis une vingtaine d'années), mais parce que Bitcoin représente un bon équilibre et une manière vraiment innovante d'atteindre un consensus économique authentique et global sur les transactions, même s'il y a beaucoup de banques Bitcoin frauduleuses et que n'importe qui peut en ouvrir une.

Bien sûr, comme pour toute monnaie, il faut acheter la monnaie avec autre chose, du travail, ou avec une autre monnaie, il y a des organismes de change qui font ça. Il existe d'autres limitations. Il faut une dizaine de minutes pour un règlement – environ dix minutes de calcul entre le moment où vous déclenchez le paiement et le moment où l'autre partie peut être assurée de l'existence d'un consensus global quant à la réalité de la transaction. C'est exactement comme pour le cash ordinaire, et on fait donc face aux mêmes problèmes de vol qu'avec le cash. Mais on bénéficie aussi de tous ses avantages : une fois que vous avez votre cash en main, vous savez que vous avez été payé, il n'y a pas de chèque qu'on peut bloquer, pas de banque qui peut rejeter la transaction. Les relations de coercition sont éliminées. D'un autre côté, il faut donc protéger le cash. Je pense que c'est le problème le plus important. Il ne serait pas très compliqué d'ajouter des niveaux, de mettre sur pied des comptes de séquestre sur lesquels on déposerait ses bitcoins, un service conçu expressément pour se protéger et s'assurer contre le vol.

JACOB : Il y a quelque chose d'intéressant : si les inventeurs de Bitcoin avaient rendu obligatoire l'utilisation de Tor – on n'aurait pas besoin d'ouvrir un compte, il suffirait de créer des identifiants cryptographiques –, donc, si tout passait par Tor en tant que noyau de base, il aurait été possible de garantir l'anonymat de lieu, même avec des identifiants à long terme qui vous reconnaîtraient de manière à pouvoir relier vos transactions.

JÉRÉMIE : Sans entrer dans les détails techniques, pourquoi ne pas dire tout simplement que

Bitcoin est une excellente idée qui a quelques défauts ? Elle est déflationniste par nature, parce que l'argent tend à disparaître de Bitcoin. Donc, ça ne peut pas marcher à long terme, mais les concepts peuvent être améliorés. On en est à la version 0.7 ou 0.8 en ce moment.

JACOB : C'est comme si on réinventait David Chaum11.

ANDY : Pour moi, Bitcoin est la tentative la plus sérieuse des dix dernières années pour introduire une monnaie numérique.

JULIAN : Le dosage des ingrédients est presque parfait. On n'a pas fini d'entendre parler de Bitcoin. C'est une monnaie efficace, on peut ouvrir un compte en quelques secondes, et le coût d'une transaction est celui de la connexion Internet plus quelques minutes de courant électrique. Comparé à toutes les autres formes de transfert d'argent, c'est très compétitif. Je pense que c'est appelé à se développer. Il suffit de voir ce qui s'est passé après plusieurs affaires de vol sur Bitcoin et leur traitement négatif dans les médias à l'été 2011 : le cours de Bitcoin est tombé à 3 dollars12. Puis il est progressivement remonté à 12 dollars. Ça ne s'est pas passé de manière brutale, il n'y a pas eu de rebond, ça a grimpé progressivement en suivant une courbe graduelle qui semble montrer l'existence d'une vraie demande. Je pense qu'une partie de cette demande est liée au trafic de drogue à petite échelle, de la marijuana par la poste et ainsi de suite13. Mais les coûts de Bitcoin en tant que monnaie sont très faibles. Divers fournisseurs d'accès ont commencé à l'utiliser, surtout dans des endroits où l'on n'a pas facilement accès aux services de cartes de crédit, comme en ex-Union soviétique.

Si l'expansion se poursuit, elle entraînera une répression. Ça ne fera pas disparaître Bitcoin, parce que la cryptographie interdit toute attaque frontale, mais les services de change qui vendent et achètent du bitcoin seront ciblés. D'un autre côté, ces services peuvent se trouver partout dans le monde, et il faudra donc tenir compte de toutes sortes de juridictions pour que ça marche, et le marché noir sera toujours là pour prendre le relais avec sa propre logique. Je pense que la voie à suivre avec Bitcoin, c'est de le faire adopter par les FAI (fournisseurs d'accès à Internet) et l'industrie des services Internet pour ces petits jeux qu'on achète sur Facebook et ainsi de suite, parce que c'est un système très performant. Une fois qu'il aura été adopté par tout un ensemble d'industries, celles-ci formeront un lobby et se battront contre son interdiction. Un peu comme ça s'est passé pour la cryptographie. Au début, on a voulu en faire une sorte de trafic d'armes, et certains d'entre nous ont été dépeints comme des marchands d'armes, mais, dès que les navigateurs l'ont adoptée pour la sécurisation des transactions bancaires en ligne, un puissant lobby s'est constitué pour empêcher son interdiction – même si l'on assiste à de nouvelles tentatives en ce moment.

JACOB : Le hic, c'est que le problème de la protection de nos données privées ne se limite pas à cette situation. Disons les choses comme elles sont. Il est tout simplement faux de prétendre que cela se passe différemment dès qu'on n'est plus sur Internet. Avant de venir ici, j'ai acheté des livres sterling, et j'ai dû fournir mon numéro de Sécurité sociale (mon identifiant unique aux États-Unis), mon nom, mes références bancaires, et de l'argent. Les numéros de série ont été dûment enregistrés, ensuite toutes ces informations ont été transmises au gouvernement fédéral. Voilà le bon point de

comparaison. Il devient difficile d'obtenir des devises aux États-Unis quand on n'est pas intégré au système. Historiquement, il a toujours existé une tendance au contrôle des changes, et elle n'est pas limitée à Internet. J'ai entendu dire que certains distributeurs dans les banques enregistrent les numéros de série des billets, ce qui permet ensuite d'analyser la circulation de l'argent, de voir où il est dépensé et qui fait quoi avec.

Si l'on compare ces systèmes avec Internet, notre migration en ligne n'a pas amélioré la protection de la vie privée – en fait, elle est restée tout aussi déplorable qu'elle l'était au départ. C'est pour ça qu'il me semble important d'analyser la situation dans le monde pré-Internet pour mieux comprendre dans quelle direction nous allons. Si vous avez de quoi payer, vous pourrez protéger votre intimité, sinon tant pis. Et Internet a aggravé les choses. Bitcoin représente peut-être un pas dans la bonne direction parce qu'en le combinant à des moyens de communication anonymes, comme Tor, vous pourrez envoyer du bitcoin à WikiLeaks, et si quelqu'un surveille cette transaction, tout ce qu'il verra, c'est qu'un utilisateur de Tor envoie un bitcoin à WikiLeaks. C'est faisable, et c'est bien mieux que l'argent liquide à certains égards.

JULIAN : La protection du caractère privé des communications, la liberté de publication, tout ça est assez facile à comprendre – il y a une longue histoire en la matière et les journalistes adorent en parler parce qu'il y va de leurs propres intérêts. Mais comparons la valeur du respect de la vie privée et celle de la liberté économique : chaque fois que la CIA observe une interaction économique, elle sait qu'il s'agit de telle personne à tel endroit et de telle autre personne à tel autre endroit, et ils attribuent un chiffre à l'interaction qui caractérise son importance à leurs yeux. On peut donc se poser la question : la liberté économique, le caractère privé des interactions économiques, n'est-ce pas en fait plus important que la liberté de parole, dans la mesure où les interactions économiques sont le fondement même de la structure sociale ?

JACOB : Elles sont intrinsèquement liées. Je pense que les cypherpunks européens et américains se distinguent sur ce point précis : les Américains pensent qu'il s'agit en gros de la même chose. Parce que dans une société de libre marché, il est vrai que l'argent et la liberté de parole vont de pair.

JULIAN : L'argent constitue le pouvoir.

JACOB : Tout à fait. Je ne prétends pas que c'est bien, c'est peut-être une attitude de droite, et ce n'est peut-être pas ce que nous souhaitons. Une sorte de capitalisme avec des contraintes sociales serait peut-être préférable, par exemple.

JULIAN : Prenons le cas d'un service de renseignements qui disposerait d'un budget de 10 millions de dollars. Ils ont le choix entre espionner les courriers électroniques des gens et surveiller étroitement leurs interactions économiques. À ton avis, qu'est-ce qu'ils choisiront ?

ANDY : Je pense qu'aujourd'hui ils diront : « Si on force les sociétés de paiement et les banques à utiliser Internet, on aura le beurre et l'argent du beurre. » C'est ce qu'ils font, d'ailleurs. Le problème est bien qu'il n'existe aucune échappatoire. On peut utiliser Tor pour protéger ses communications, on peut crypter ses appels téléphoniques, on peut envoyer des SMS ou chatter de manière sécurisée. Mais, pour l'argent, c'est bien plus compliqué, sans compter toutes les lois antiblanchiment, et le discours général sur les trafiquants de drogue et les terroristes qui profitent de l'infrastructure pour faire des choses horribles.

JACOB : Deux des quatre Cavaliers de l'Infocalypse.

ANDY : En fait, il faudrait que les organismes de surveillance et les dépenses des États en la matière soient transparents. La question est : que se passerait-il si l'anonymat était accordé au système financier ? À quel résultat aboutirait-on ? Ce serait intéressant : certaines personnes se sentiraient plus libres et diraient : « Je peux hausser la voix, je peux m'adresser au Parlement, mais je peux aussi acheter quelques hommes politiques. »

JÉRÉMIE : Tu penses à ce qui se passe aux États-Unis, n'est-ce pas ?

JACOB : Mais il n'y a pas d'anonymat.

ANDY : Je ne suis pas certain que ça se limite aux États-Unis. En Allemagne, il existe des fondations qui acquièrent des tableaux peints par les épouses d'hommes politiques, on n'appelle pas ça de la corruption, ça se passe sur le marché de l'art et d'autres secteurs. Nous avons trouvé des noms plus acceptables pour ces pratiques. En France, je ne sais pas, ça s'appelle peut-être « soirée entre amis », tandis qu'ailleurs on fait appel à des call-girls.

JÉRÉMIE : Le cas des États-Unis est spécial parce qu'il existe des liens très étroits entre le système politique et l'argent. Après dix ans passés à batailler sur les questions de copyright, Larry Lessig a annoncé qu'il laissait tomber (en vérité, il ne l'a pas fait) parce qu'il a compris que le problème ce ne sont pas les idées néfastes des hommes politiques en matière de copyright, mais les liens innombrables qui existent entre eux et les acteurs industriels qui défendent ces idées néfastes14. C'est un vrai problème.

JULIAN : Tu es certain que c'est un problème, Jérémie ? Après tout, c'est peut-être une bonne chose que ces industries si productives...

ANDY : Je crois que l'avocat du diable est en train de boire mon whisky.

JACOB : Voyons s'il peut finir sa phrase sans se marrer. Faites donc le troll, maître Troll.

JULIAN : Les industries productives, celles qui génèrent une richesse dont bénéficie l'ensemble de la société, consacrent une partie de leur argent à s'assurer qu'elles pourront maintenir cette productivité, en s'opposant aux tentatives de législation qui surgissent quand la tendance du moment remet au goût du jour certains mythes fondateurs de la politique. Or, la meilleure manière d'y parvenir, c'est d'acheter des membres du Congrès, de se servir du fruit du travail de leurs industries productives pour modifier la loi et, par là même, s'assurer qu'il ne sera pas porté atteinte à leur productivité.

JACOB : Attendez, laissez-moi répondre. Vous êtes prêts ? Vous êtes prêts ? Là, tout de suite ? Non.

JULIAN : Quel est le problème ?

JACOB : Il y en a plusieurs, à commencer par le feed-back négatif qui se met en place. Par exemple, un des plus importants donateurs politiques en Californie est le syndicat des gardiens de prison. Et ils font du lobbying pour des lois plus dures non parce qu'ils se soucient du maintien de la paix sociale, mais parce que cela favorise l'emploi dans leur secteur15. Ces gens font des pieds et des mains pour qu'on construise davantage de prisons et qu'on y enferme encore plus de gens, que leur peine soit plus lourde, etc. Or, dans les faits, cela revient simplement à se servir de l'argent qu'ils reçoivent pour un travail utile – parce qu'il l'est – afin d'élargir un monopole qui leur a été concédé par l'État.

JULIAN : Tu veux dire qu'ils l'utilisent pour transférer la richesse d'industries productives vers des industries qui ne le sont pas ?

JACOB : On pourrait dire les choses comme ça.

JULIAN : C'est peut-être un phénomène minoritaire. Tout système engendre des abus, et il y a toujours un petit groupe de malins pour en profiter. Mais peut-être que l'essentiel du lobbying, la majeure partie des pressions qui s'exercent sur le Congrès est le fait d'industries productives qui cherchent simplement à faire en sorte que la loi ne les empêche pas de le rester.

JACOB : On peut mesurer tout ça très facilement, il suffit de regarder quels lobbies cherchent à protéger les situations de rente, à empêcher autrui de créer des situations susceptibles de remettre en cause leur position de domination. Ce type de comportement montre que quelque chose cloche profondément : on se contente de protéger des acquis, acquis obtenus pour l'essentiel par l'exploitation éhontée de réactions émotionnelles, style : « Mon Dieu, il faut stopper le terrorisme, la pornographie infantile, le blanchiment d'argent, il faut faire la guerre à la drogue. » Ce qui était sans doute tout à fait raisonnable dans le contexte de départ parce que nous avons tendance à penser qu'il s'agit de choses néfastes, et de problèmes sérieux.

ANDY : J'aimerais revenir à la question du copyright pour vous donner un autre exemple : l'invention de l'automobile a suscité de grands débats. Les compagnies de transport à cheval craignaient que cela signe la fin de leurs activités, ce qui était vrai mais pas forcément mauvais. Un jour, on m'a invité à parler devant l'association des sociétés de cinéma allemandes. Avant moi un professeur de l'université de Berlin avait évoqué en des termes on ne peut plus policés l'évolution de l'espèce humaine et son développement culturel, l'idée étant en gros que la reproduction de pensées et leur traitement ultérieur en est l'élément clé, un peu comme quand le cinéma reprend des thèmes en les exprimant d'une manière dramatique. Après une quarantaine de minutes, le modérateur l'a interrompu assez sèchement et lui a dit : « Donc après ce que vous venez de dire nous devrions légaliser le vol. Je suis curieux de voir ce qu'en pense le gars du Chaos Computer Club. » J'ai pensé : « Putain ! Si je dis ce que je pense, ils vont me manger tout cru ! » Donc, certaines industries reposent sur des modèles qui sont à l'opposé de l'évolution naturelle. C'est égoïste, cette manière de rester sur cette ligne anti-évolutionniste, de la rendre encore plus monopolistique. Quand on a inventé les minicassettes, on a aussi dit que c'était la fin de l'industrie musicale. C'est exactement l'inverse qui s'est produit, l'industrie a connu une expansion incroyable. Ma question est : quelle est la bonne politique dans ce cas ? Quelle est la bonne manière de formuler ces enjeux ?

JULIAN : Je me demande si on ne pourrait pas, en fait, standardiser la pratique américaine, juste la formaliser pour qu'on puisse tout bonnement acheter des sénateurs et des voix au Sénat.

JÉRÉMIE : Non, non, non, non.

ANDY : OK, suppose que nous ayons l'argent.

JULIAN : Oui, et que tout soit transparent et qu'il y ait des acheteurs, et des vendeurs, et des enchères.

ANDY : L'industrie de l'armement aura quand même toujours plus d'argent que quiconque.

JULIAN : Pas forcément. Je pense que le complexe militaro-industriel se trouverait marginalisé dans une certaine mesure parce que sa capacité à opérer derrière des portes closes, dans un système sans enchères généralisées ouvertes, est plus importante que celle d'autres industries.

JACOB : Le système est foncièrement inégal.

JÉRÉMIE : D'un point de vue économique libéral, antimonopolistique, quand on dit : « Laissons les acteurs dominants décider de la politique à suivre », que se passe-t-il ? Je vous renvoie à l'expérience d'Internet au cours des quinze dernières années : l'innovation s'est fait essentiellement de bas en haut, comme on dit, et de nouvelles pratiques sont nées de rien, genre deux types dans un garage qui ont inventé une technologie qui s'est diffusée.

JULIAN : Ça s'est passé comme ça pour presque tout le monde, Apple, Google, YouTube, tout.

JÉRÉMIE : Absolument. Tout ce qui s'est produit pour Internet est resté sous les radars pendant des mois ou des années avant d'exploser au grand jour, alors il est impossible de prédire quelle sera la prochaine innovation, et le tempo est trop rapide, infiniment plus rapide que le processus de prise de décision politique. Donc, si tu votes une loi qui a un effet sur le marché tel qu'il est aujourd'hui, ou sur le rapport de force entre différentes compagnies et acteurs, si tu renforces ce qui existe déjà, tu interdiras peut-être à un nouvel arrivant hyperperformant d'émerger.

JULIAN : Pour être libre, le marché doit être régulé.

JÉRÉMIE : Il faut évidemment combattre les monopoles, et il faut un pouvoir plus grand que celui de ces entreprises pour punir les mauvais joueurs. Mais le plus important à mes yeux, c'est que la politique doit s'adapter à la société, et non l'inverse. La guerre du copyright donne le sentiment que le législateur essaie de contraindre l'ensemble de la société à adopter un cadre défini par Hollywood : « OK, vos nouvelles pratiques culturelles sont moralement répréhensibles, donc si vous vous obstinez, nous mettrons au point des instruments juridiques pour vous contraindre à faire ce qui nous semble juste. » Ce n'est pas en procédant comme cela que l'on aboutit à des politiques valables. Une bonne politique doit tenir compte de ce qui se passe dans le monde et s'adapter de manière à contrecarrer ce qui est mauvais et appuyer ce qui est bien. Je suis persuadé que lorsqu'on laisse les acteurs industriels les plus puissants décider de la politique à suivre, cela ne se passe pas comme ça.

ANDY : J'essaie juste d'aborder positivement ce qui définirait une bonne politique. Ce que tu viens

de dire est un peu trop compliqué pour moi. Je préfère davantage de simplicité. Heinz von Foerster, un des pères de la cybernétique, a défini un ensemble de règles, dont une disait : « Agissez toujours de manière à élargir le champ de vos options16. » Ça s'applique à la politique, à la technologie, à tout ce que vous voudrez. Faites toujours ce qui élargira vos choix, pas l'inverse.

JULIAN : Ça marche aussi pour les échecs.

ANDY : Une protection accrue de la vie privée en matière de transactions financières peut avoir un effet négatif. Posons la question de la manière suivante : « Le système monétaire actuel a sa propre logique, comment fait-on pour interdire qu'elle se généralise à d'autres domaines ? » Car, à l'inverse des télécommunications, le système monétaire peut influer sur les options d'autrui en les limitant totalement. Si vous avez la possibilité d'engager des tueurs à gages pour accomplir certaines choses précises, si vous pouvez acheter des armes pour faire la guerre à d'autres pays, alors vous restreignez les options dont disposent d'autres personnes en ce qui concerne leur vie, leurs actions. En mettant plus d'argent dans les communications, j'augmente les possibilités des gens. En revanche, en mettant plus d'armes sur le marché...

JACOB : Pas d'accord – plus tu améliores tes capacités de surveillance, plus tu contrôles les gens.

ANDY : C'est un argument de plus en faveur du contrôle du marché de l'armement, dont font partie les technologies de surveillance des communications.

JACOB : Ben voyons, tu veux restreindre ma capacité à vendre ça, d'accord, mais comment fais-tu ? Comment limites-tu ma capacité à transférer de la richesse ? Grâce aux réseaux de communication. L'une des choses les plus choquantes dans le sauvetage des banques américaines – qui était choquant à bien d'autres égards pour toutes sortes de raisons –, c'est qu'on a vu que la richesse n'est rien d'autre que des bits dans le système informatique. En faisant pression d'une manière particulièrement efficace, certaines personnes ont réussi à obtenir que leurs bits soient cotés au plus haut, et ça soulève tout de suite une question : que vaut ce système, s'il vous permet de tricher pour que tous vos bits soient cotés au plus haut ? Les bits des pauvres gens qui se retrouvent dans la merde, en revanche, sont passés par pertes et profits17.

ANDY : Si je comprends bien, selon toi nous avons besoin d'un système économique totalement différent ? Parce que aujourd'hui la valeur n'est pas définie par la valeur économique.

JACOB : Non, je dis qu'il existe une valeur économique.

ANDY : Tu peux faire de mauvaises choses et gagner beaucoup d'argent, et tu peux en faire de bonnes et ne pas en tirer un centime.

JACOB : Ce que je veux dire, c'est que tu ne peux pas dissocier l'économie des moyens de communication. Je ne sais pas s'il faut changer de système économique. Je ne suis pas économiste. Je pense que les systèmes de communication, avec leur liberté, possèdent une certaine valeur, et que la liberté de l'échange possède aussi une certaine valeur : j'ai le droit de te donner quelque chose en échange de ton travail, tout comme j'ai le droit de t'expliquer une idée et tu as le droit de me dire ce que tu penses de mon idée. Le système économique n'existe pas dans une sorte de néant. Le système de communication y est directement relié, et cela fait partie du tissu même de la société.

Si l'on veut adopter une vision réductionniste de la liberté – les trois libertés mentionnées par Julian –, c'est évidemment lié à la liberté de mouvement : si tu cherches à acheter un billet d'avion sans utiliser un moyen de paiement traçable, tu te feras signaler. Si tu te présentes au guichet et que tu essaies d'acheter cash un billet pour le jour même, tu seras signalé. On te fera subir des vérifications de sécurité supplémentaires, tu ne peux pas voler sans pièce d'identité et si tu as le malheur d'acheter ton billet avec une carte de crédit, ils conserveront toutes les traces te concernant, de ton adresse IP au type de navigateur que tu utilises. En invoquant le Freedom of Information Act, j'ai réussi à me faire communiquer par les douanes et l'immigration toutes les données me concernant sur une période de deux ou trois ans. Je m'étais dit que ce serait intéressant d'y jeter un œil. J'y ai trouvé le nom de Roger Dingledine, qui m'a acheté un jour un billet d'avion pour un truc de boulot, avec sa carte de crédit, l'endroit où il se trouvait quand il a acheté le billet, le navigateur qu'il avait utilisé, tout ce qui concernait ce billet d'avion était là.

JULIAN : Et tout ça avait été transmis au gouvernement américain, ou ils s'étaient contentés de le conserver dans leur base de données ?

JACOB : Ils avaient tout transmis. Les données avaient été rassemblées, reliées entre elles, et transmises au gouvernement fédéral. Ce que je trouve complètemet dingue, c'est qu'il s'agit de la fusion des trois choses dont tu parles. Mon droit de voyager librement, mon droit d'acheter ce billet d'avion ou de le faire acheter par quelqu'un, et mon droit à la parole – je devais prendre la parole quelque part et, pour honorer cet engagement, j'ai dû faire des concessions dans les deux autres sphères. Cela influe donc bien sur ma liberté de parole, encore plus lorsque je découvre que toutes ces données ont été rassemblées et reliées.

1. Sur cette question, on peut trouver toutes sortes d'éléments fascinants dans les télégrammes diplomatiques américains divulgués par WikiLeaks. Voir par exemple, pour une discussion plus détaillée, les télégrammes suivants (identifiés par leurs références, liens vérifiés le 24 octobre 2012) :

07BEIRUT1301 : http://wikileaks.org/cable/2007/08/07 BEIRUT1301.html

08BEIRUT490 : http://wikileaks.org/cable/2008/04/08 BEIRUT490.html

08BEIRUT505 : http://wikileaks.org/cable/2008/04/08 BEIRUT505.html

08BEIRUT523 : http://wikileaks.org/cable/2008/04/08 BEIRUT523.html

2. Voir télégramme référence n° 10MOSCOW228, WikiLeaks : http://wikileaks.org/cable/2010/02/10 MOSCOW228.html (lien vérifié le 24 octobre 2012).

3. Pour plus de détails sur l'assassinat des citoyens américains Anwar al-Awlaki et de son fils Abdulrahman al-Awlaki, voir Glenn Greenwald, « The due-process-free assassination of U.S. citizens is now reality », Salon, 30 septembre 2011 : http://www.salon.com/2011/09/30/awlaki_6. Ainsi que « The killing of Awlaki's 16-year-old son », Salon, 20 octobre 2011 :

http:// www.salon.com/2011/10/20/the_killing_of_awlakis_16_year_old_son.

« Il est littéralement impossible d'imaginer une répudiation plus brutale des fondements mêmes de la République que le développement d'une branche secrète, libre de tout contrôle, qui collecte des informations sur des citoyens et applique ensuite une "matrice de disposition" pour décider quel châtiment devra être appliqué. C'est une dystopie politique classique devenue réalité », Glenn Greenwald, « Obama moves to make the War on Terror permanent », Guardian, 24 octobre 2012 : http://www.guardian.co.uk/commentisfree/2012/oct/24/obama-terrorism-kill-list (tous ces liens ont été vérifiés le 24 octobre 2012).

4. Pour plus de détails, voir The Anonymity Bibliography, Selected Papers in Anonymity, sous la direction de Roger Dingledine et Nick Mathewson : http://freehaven.net/anonbib (lien vérifié le 24 octobre 2012). Les monnaies chaumiennes sont émises de manière centralisée, mais utilisent la cryptographie pour garantir l'anonymat des transactions. De ce point de vue, les monnaies chaumiennes se distinguent de Bitcoin, une autre monnaie électronique discutée plus loin en détail, dans laquelle toutes les transactions sont publiques, mais pour laquelle il n'existe pas d'autorité centrale.

5. Pour davantage de détails sur le blocus bancaire contre WikiLeaks, voir le chapitre « À propos des diverses tentatives de persécution de WikiLeaks et des individus qui y sont associés ».

6. Julian fait ici référence aux plans du gouvernement britannique pour généraliser l'utilisation du traçage électronique. Voir : « Over 100,000 offenders to be electronically tagged », Guardian, 25 mars 2012 : http://www.guardian.co.uk/society/2012/mar/25/prisons-and-probation-criminal-justice (lien vérifié le 22 octobre 2012). Au moment où avait lieu la discussion, Julian était encore aux arrêts domiciliaires en attendant le jugement concernant sa demande d'extradition. Après son placement en isolement sans inculpation au mois de décembre 2010, la détention de Julian a été

transformée en arrêts domiciliaires contre le versement d'une caution de plus de 300 000 livres sterling. Selon les termes de sa peine, il devait se trouver à une certaine adresse à certaines heures, ce régime étant mis en œuvre grâce à l'utilisation d'un bracelet de surveillance fixé à sa cheville, géré par une firme privée de sécurité travaillant sous contrat du gouvernement britannique. Les déplacements de Julian ont été limités pendant plus de 550 jours par le fait qu'il devait se présenter quotidiennement à la police, à une heure donnée. Au moment où paraît ce livre, Julian se trouve à l'ambassade d'Équateur à Londres, qui est encerclée jour et nuit par la police londonienne. Au mois de juin 2012, Julian s'y est présenté pour demander l'asile politique, arguant de la persécution dont il fait l'objet par le gouvernement des États-Unis et ses alliés. L'asile politique lui a été accordé au mois d'août 2012.

7. « Is CCA Trying to Take Over the World ? » American Civil Liberties Union, 21 février 2012 : http://www.aclu.org/blog/prisoners-rights/cca-trying-take-over-world. « Passing House Bill will worsen already pressing civil rights issue », ANNARBOR.com, 2 août 2012 : http://annarbor.com/news/opinion/passing-house-bill-will-worsen-already-pressing-civil-rights-issue. Voir aussi « Goldman Sachs to invest $9.6m in New York inmate rehabilitation », Guardian, 2 août 2012 : http://www.guardian.co.uk/society/2012/aug/02/goldman-sachs-invest-new-york-jail (tous ces liens ont été vérifiés le 24 octobre 2012).

8. Bitcoin (http://bitcoin.org) est la première implémentation réussie d'un concept cypherpunk classique : la monnaie numérique cryptographique. Bitcoin est évoqué en détail un peu plus loin, mais on trouve une excellente explication générale de la technologie et de la philosophie sous-jacentes dans « Understanding Bitcoin », Al Jazeera, 9 juin 2012 : http://www.aljazeera.com/indepth/opinion/ 2012/05/20125309437931677.html (lien vérifié le 22 octobre 2012).

9. e-gold était une monnaie numérique – et une entreprise – lancée en 1996. Les propriétaires ont été inculpés par le département américain de la Justice de « conspiration en vue d'opérations de blanchiment d'argent ». Ils ont plaidé coupables et ont été condamnés à des peines de prison avec sursis, d'arrêts domiciliaires et de travaux d'intérêt général. Le juge a déclaré qu'ils ne méritaient pas de peines plus lourdes car il n'était pas dans leur intention de se livrer à des activités illégales. Voir « Bullion and Bandits: The Improbable Rise and Fall of E-Gold », Wired, 9 juin 2009 : http://www.wired.com/threatlevel/2009/06/e-gold (lien vérifié le 22 octobre 2012).

10. Avant Internet, le réseau X.25 était le plus grand réseau global d'échange de données existant, avec le réseau téléphonique. La facturation sur X.25 dépendait des quantités de données émises et reçues, non de la durée d'une connexion comme sur le réseau téléphonique. Les portails (appelés des PAD) permettaient de se connecter au réseau X.25 à partir du réseau téléphonique grâce à des modems ou des coupleurs acoustiques. Pour plus de détails voir Wikipédia : http://fr.wikipedia.org/wiki/X.25 (lien vérifié le 24 octobre 2012).

11. David Chaum est cryptographe et inventeur de protocoles cryptographiques. Pionnier des

technologies monétaires, il a inventé eCash, l'une des premières monnaies anonymes cryptographiques.

12. Sur l'effet des articles négatifs, voir « Bitcoin implodes, falls more than 90 percent from June peak », Arstechnica, 18 octobre 2011 : http://ars-technica.com/tech-policy/2011/10/bitcoin-implodes-down-more-than- 90-percent-from-june-peak (lien vérifié le 22 octobre 2012).

13. Voir, par exemple, « The Underground Website Where You Can Buy Any Drug Imaginable », Gawker, 1er juin 2011 : http://gawker.com/5805928/ the-underground-website-where-you-can-buy-any-drug-imaginable (lien vérifié le 22 octobre 2012).

14. Les travaux précurseurs de Lawrence Lessig sur le droit d'auteur et la culture (par exemple dans son livre Free Culture, New York, The Pinguin Press, 2004) ont laissé la place ces dernières années à un intérêt pour la corruption de la démocratie américaine par le lobbying parlementaire. Voir le wiki Lessig : http://wiki.lessig.org.

15. Le California Correctional Peace Officers Association est un groupe californien influent qui fait régulièrement don de millions de dollars lors de campagnes électorales, même s'il n'est pas toujours le donateur le plus important. Voir « California reelin », The Economist, 17 mars 2011 : http://www.economist.com/node/18359882. Et « The Golden State's Iron Bars », Reason, juillet 2011 : http://reason.com/archives/2011/ 06/23/the-golden-states-iron-bars. Voir aussi l'entrée « California Correctional Peace Officers Association » sur le site Web FollowThe Money du National Institute for Money in State Politics : http://www.followthemoney.org/database/topcontributor.phtml?u=3286&y=0 (tous les liens ont été vérifiés le 22 octobre 2012).

16. Heinz von Foerster (1911-2002) était un scientifique austro-américain et un des architectes de la cybernétique. Son « impératif éthique » est : « Agissez toujours de manière à accroître le nombre de vos choix. » En allemand : « Handle stets so, daß die Anzahl der Wahlmöglichkeiten größer wird. »

17. Jacob attribue cette observation à John Gilmore.

Censure

JULIAN : Jacob, raconte-nous un peu le harcèlement dont tu as fait l'objet dans les aéroports

américains, et la raison pour laquelle tu subis tout ça.

JACOB : Quand je pose la question, on me répond que je sais bien pourquoi.

JULIAN : On ne te donne pas de motif plus précis ?

ANDY : Je voudrais essayer de résumer la situation. La sécurité technique et la sécurité des affaires gouvernementales sont deux choses entièrement distinctes. Ton système technique peut être totalement sécurisé et ça déplaira au gouvernement parce que, de son point de vue, la sécurité c'est pouvoir observer ce qui se passe, contrôler ce qui se passe, et donc pouvoir violer la sécurité technique. Le but n'est pas d'empêcher Jacob de monter dans un avion pour tuer des gens, ou le détourner, ou n'importe quoi d'autre. Le but est d'emmerder cet empêcheur de tourner en rond qui voyage à l'étranger, parle à des gens, diffuse ses idées. Après tout, ce qui peut arriver de pire à un gouvernement de nos jours, c'est que les gens puissent avoir de meilleures idées que la politique qu'il mène.

JACOB : Je suis très touché par tous ces compliments, mais en fait ça va bien plus loin : les données qu'ils recueillent sont celles de Monsieur Tout-le-monde. Ça a commencé bien avant que je fasse quoi que ce soit de gênant pour eux. Le simple fait de voyager et l'existence de ces systèmes avec cette architecture permettaient déjà de rassembler ces informations. C'était bien avant qu'on ne m'arrête pour un oui ou pour un non, bien avant qu'on ne m'expulse du Liban, bien avant que le gouvernement américain s'intéresse à mon cas particulier.

ANDY : Ils l'avaient peut-être prévu, ils l'ont peut-être vu venir avant toi.

JACOB : J'en suis convaincu, et sans doute parce qu'ils collectaient déjà ces informations. Mais on ne me répond jamais deux fois la même chose. La réponse de base est : « C'est comme ça, on est dans notre droit. » Moi, je leur réponds : « D'accord, je ne conteste pas votre autorité – en fait, si, mais bon, pas là, tout de suite –, j'aimerais juste qu'on m'explique pourquoi on me fait subir ça. » On n'arrête pas de me dire : « Mais enfin, Jacob, c'est évident, non ? Tu travailles sur Tor », ou bien : « Tu es proche de Julian, qu'est-ce que tu t'imagines ? » Je trouve ça sidérant, parce que les gens qui me font subir ça, c'est-à-dire les services des douanes, la police aux frontières et les services d'immigration américains, me disent, eux, que c'est surtout parce qu'ils en ont le droit. J'ai aussi réussi à leur faire dire des conneries dans le genre : « Vous vous souvenez du 11-Septembre ? C'est à cause de ça », ou bien : « On veut vous poser des questions, et selon nous, dans ce cadre, vos droits sont limités. »

On m'interdit de me faire assister par un avocat, on m'empêche d'aller aux toilettes tout en me donnant à boire un truc qui est un genre de diurétique à mon avis, le tout pour essayer de me forcer à coopérer. On fait ça pour me mettre la pression pour des raisons politiques. On m'a demandé ce

que je pensais de la guerre en Irak, de la guerre en Afghanistan. En gros, d'un bout à l'autre, on use à mon égard des mêmes procédés que le FBI pendant l'opération Cointelpro (le programme d'espionnage intérieur généralisé qui a fonctionné de 1956 à 1971). Par exemple, ils ont expressément essayé de jouer de leur autorité pour modifier ma vision politique de la réalité, ils ont fait pression sur moi pas seulement pour que je la change, mais pour que je leur donne les clés de compréhension de ma façon de penser. On a saisi certaines de mes affaires. Je n'ai pas vraiment le droit de raconter tout ce qui m'est arrivé parce que c'est une zone grise, je ne sais même pas si j'ai le droit de mentionner que tout ça m'est arrivé. Je suis sûr que je ne suis pas le seul, mais je n'ai jamais entendu personne en parler.

Un jour, j'étais à l'aéroport de Toronto, je rentrais à la maison après avoir rendu visite à ma famille. Je devais m'envoler pour Seattle, où j'habitais à l'époque, et on m'a arrêté, on m'a fait attendre dans une première zone de rétention, puis dans une deuxième, puis dans une troisième, et enfin dans une cellule. Je suis resté tellement longtemps que, lorsqu'ils m'ont finalement libéré, mon avion était parti. La chose curieuse, c'est que ces zones de prédétention sont en fait, d'un point de vue technique, des territoires américains sur le sol canadien, et il existe une règle selon laquelle si vous ratez votre avion, ou s'il vous faut attendre un certain temps le vol suivant, alors on doit vous laisser partir. Donc, techniquement, je me suis fait jeter des États-Unis pour avoir été détenu trop longtemps et j'ai dû entrer de nouveau au Canada, prendre un vol jusqu'à l'autre bout du pays, puis franchir la frontière au volant d'une voiture de location. Mais devinez quoi, à la frontière on m'a dit : « Combien de temps êtes-vous resté au Canada ? » J'ai répondu : « Eh bien, cinq heures plus le temps que j'ai passé en détention à Toronto », et comme j'étais resté au Canada environ huit heures, on m'a dit : « Bienvenue à la maison, on va vous arrêter de nouveau. » Ils ont démonté la voiture, ils ont démonté mon ordinateur, ils ont fouillé partout, et ils m'ont placé en détention. Ils ont été très charitables : après une demi-heure, ils m'ont permis d'aller aux toilettes. C'est ce qu'on appelle l'exception des fouilles à la frontière – ils font ça parce qu'ils affirment avoir le droit de le faire, et personne ne s'y oppose1.

JULIAN : OK, on voit bien ce qui t'est arrivé, mais quand mes contacts chinois parlent du grand pare-feu de Chine – en Occident on dit que c'est de la censure, parce que l'on interdit aux citoyens chinois de lire ce qui s'écrit à l'extérieur sur leur gouvernement, ce que disent les dissidents, Falun Gong et la BBC, et aussi, pour être tout à fait honnête, la propagande contre la Chine –, eux, ce n'est pas la censure qui les inquiète le plus. Ce qui les inquiète le plus, c'est la surveillance extrême d'Internet sur laquelle repose cette censure. Pour vérifier ce que regarde Untel, pour savoir s'il fait quelque chose d'interdit ou non, il faut qu'on sache qui c'est, donc que quelqu'un le surveille et enregistre ses gestes. Ça a l'effet d'une douche froide sur les Chinois – pas tant le fait qu'on les censure, mais qu'on épie le moindre de leurs gestes. En fait, ça s'applique à nous tous. Ça vous change, dès que vous en êtes conscient. Ça modifie votre comportement, on met moins d'entrain à se plaindre des autorités.

JACOB : Pourtant, c'est justement la manière dont il ne faut pas réagir à ce type d'intrusion. Le harcèlement que je subis aux frontières, par exemple, n'a rien d'exceptionnel, tout Arabo-Américain peut en attester depuis le 11-Septembre, et même avant. Mais je refuse de ne pas exploiter le privilège d'avoir la peau blanche et un passeport américain, et je refuse de me taire, parce que ce qu'ils font est mal, et ils usent et abusent de leurs pouvoirs. Nous devons nous y opposer, tout comme des Chinois courageux s'y opposent, à l'instar d'Isaac Mao, par exemple2. Isaac milite activement et efficacement contre ce type de censure, parce que la bonne réponse n'est pas de céder à la pression simplement parce que le gouvernement dit qu'il est dans son droit.

JÉRÉMIE : Nous voici donc rattrapés par la politique, parce que tu dis en gros que les gens doivent se battre pour leurs droits – mais les gens ont besoin qu'on leur explique pourquoi c'est nécessaire, et pour cela ils doivent pouvoir communiquer. Il m'est arrivé de discuter avec des Chinois – je ne sais pas si c'étaient des apparatchiks, s'ils avaient été sélectionnés avant d'avoir le droit de sortir du pays et de discuter avec moi –, mais quand j'évoquais la question de la censure sur Internet, ils répondaient souvent : « Mais c'est pour le bien du peuple. La censure existe, certes, mais s'il n'y avait pas de censure, il y aurait des comportements extrémistes, on verrait des choses dont personne ne veut, alors le gouvernement prend ces mesures pour que tout se passe bien. »

JACOB : Ça ressemble à l'argument qu'ils invoquent pour justifier la collecte d'organes chez les condamnés à mort. « Il ne faut pas gâcher ces organes ! »

JÉRÉMIE : Vu la manière dont fonctionne la censure en Chine, d'un point de vue technique ça doit être un des systèmes les plus perfectionnés au monde...

JACOB : Tout à fait.

JÉRÉMIE : Et j'ai entendu dire que sur Weibo – l'équivalent chinois de Twitter – le gouvernement a la possibilité de filtrer certains hashtags et de leur interdire de sortir d'une province donnée.

JACOB : Il est important de souligner que lorsque les gens parlent de la censure en Asie, ils le font souvent en termes d'« ailleurs », comme si cela n'arrivait que « là-bas ». Or, lorsque vous faites une recherche sur Google aux États-Unis, certains résultats de recherche sont exclus en raison de ce qu'ils appellent des « contraintes légales ». Il y a une différence entre les deux choses – tant du point de vue de leur implémentation et, bien évidemment, de la réalité sociale du comment, du pourquoi et même du où –, mais une grande partie de tout ça est inscrit dans l'architecture. Dans le cas de l'Internet américain, par exemple, qui est très décentralisé, il serait très difficile de faire de la censure à la chinoise.

JULIAN : Une bonne partie de tout ça, c'est Google, et on peut censurer Google. Beaucoup de pages qui référencent WikiLeaks sont censurées par Google.

JACOB : Oui, ça ne fait pas de doute. Mais en fait, puisque l'indexation est libre, on peut en faire une analyse comparée.

JULIAN : Oui, en théorie.

JACOB : En théorie. Et aussi en pratique, puisque des gens identifient et analysent les différences entre les systèmes de censure en vigueur à travers le monde. La censure et la surveillance ne se passent pas « ailleurs ». En Occident, les gens disent souvent que « les Iraniens et les Chinois et les Nord-Coréens ont besoin d'anonymat et de liberté, mais ici on n'en a pas besoin ». Et « ici », en général, ça veut dire « aux États-Unis ». Mais en fait distinguer les régimes répressifs et les autres n'est pas le bon prisme de lecture parce que si vous faites partie de l'élite du régime, quel qu'il soit, vous ne vous sentirez pas oppressé. On considère que le Royaume-Uni est un endroit merveilleux ; en général, les gens pensent que la Suède est aussi un endroit assez génial, toutefois si les gens au pouvoir vous ont dans le nez, votre situation devient tout de suite moins agréable.

Mais bon, après tout, Julian est encore en vie, n'est-ce pas ? Donc c'est quand même un signe clair qu'il s'agit d'un pays libre – vous ne trouvez pas ?

JULIAN : J'ai travaillé dur pour aboutir à ma situation actuelle. Mais peut-être devrions-nous parler de la censure sur Internet en Occident. C'est très intéressant. Autrefois, la Grande Encyclopédie soviétique était distribuée partout. Et elle subissait des modifications en fonction des changemens politiques. En 1953, Beria, le chef de la police secrète, est tombé en disgrâce et a été exécuté. L'article le concernant, qui parlait de lui en des termes élogieux, a été retiré par la direction de l'Encyclopédie, qui a publié une modification collée dans tous les exemplaires de l'Encyclopédie. C'était assez peu discret. Je cite cet exemple parce qu'il était énorme, visible, et que cette tentative est restée dans l'histoire. Au Royaume-Uni, nous avons le Guardian et d'autres quotidiens importants qui suppriment secrètement des articles de leurs archives Internet, sans fournir la moindre explication. Si vous faites une recherche, par exemple, sur l'affaire de fraude du milliardaire Nadhmi Auchi, vous tomberez sur « Page introuvable ». Elles ont aussi été retirées des index.

Laissez-moi vous raconter comment j'en suis venu à m'intéresser à l'histoire de Nadhmi Auchi. En 1990, l'invasion du Koweït par l'Irak a déclenché la première guerre du Golfe. Le gouvernement koweïtien, d'abord en exil puis à son retour, avait besoin de liquidités, et il a donc décidé de vendre divers biens, dont plusieurs raffineries situées en dehors du pays. Un homme d'affaires britannique, Nadhmi Auchi, un Irakien qui après avoir été une figure du régime de Saddam Hussein s'était installé en Grande-Bretagne au début des années 1980, a servi d'intermédiaire et a été accusé par la suite d'avoir distribué 118 millions de dollars en pots-de-vin. Cela a donné lieu à la plus grande investigation pour fraude financière en Europe depuis la fin de la Seconde Guerre mondiale. En 2003, Auchi a été condamné pour fraude dans le cadre de l'affaire Elf. Il possède néanmoins aujourd'hui près de 200 sociétés par l'intermédiaire de ses holdings au Luxembourg et au Panamá. Il a été impliqué dans l'attribution de contrats de téléphonie mobile en Irak après la guerre, et a de nombreuses affaires à travers le monde3.

Aux États-Unis, Tony Rezko, un collecteur de fonds pour Barack Obama quand celui-ci faisait campagne pour le Sénat, était une vieille accointance d'Auchi, lequel s'était occupé de ses finances. Auchi et Rezko étaient aussi des proches de l'ex-gouverneur de l'Illinois Rod Blagojevich. Rezko et Blagojevich ont été condamnés pour corruption. Rezko en 2008 et Blagojevich en 2010-2011 (après que le FBI a enregistré une conversation téléphonique où il essayait de monnayer le siège de

sénateur d'Obama). En 2007-2008, lorsque Obama faisait campagne pour la primaire démocrate, la presse américaine a commencé à enquêter sur ses relations et ses réseaux. Ils se sont intéressés à Rezko et ont conclu que les deux hommes avaient noué des liens au moment où Obama avait acheté sa maison. En 2008, peu avant son procès, Rezko a reçu un virement de 3,5 millions de dollars de la part d'Auchi, dont il n'a pas fait état au tribunal en dépit de l'obligation qui lui en était faite – et il a atterri en prison. La presse américaine s'est alors intéressée à Auchi, et celui-ci a demandé à ses avocats britanniques, Carter-Ruck, de mener une campagne agressive au sujet de la condamnation dont il avait fait l'objet en France dans le cadre de l'affaire Elf, campagne qui a été couronnée de succès. Il a ciblé la presse britannique et même des blogs américains, et obtenu la suppression d'une bonne douzaine d'articles, vraisemblablement. La plupart de ces articles, y compris ceux qui se trouvaient dans les archives Internet de journaux britanniques, ont tout bonnement disparu. C'est comme s'ils n'avaient jamais existé. Personne n'a dit : « Suite aux injonctions des représentants légaux de M. Auchi nous avons décidé de retirer les articles. » Ils ont aussi disparu de tous les index. WikiLeaks les a retrouvés et publiés à nouveau4.

JACOB : Ils ont effacé l'histoire.

JULIAN : L'histoire n'est pas simplement modifiée, elle n'a jamais existé. C'est le dictum d'Orwell : « Qui contrôle le présent contrôle le passé, et qui contrôle le passé contrôle l'avenir. » C'est l'effacement indétectable de l'histoire en Occident, et en l'occurrence il s'agit d'une censure postpublication. L'autocensure prépublication est bien plus extrême et souvent difficile à mettre en évidence. On a pu le voir au moment du Cablegate : WikiLeaks travaillant avec différents journaux à travers le monde, nous avons pu vérifier lesquels censuraient notre matériel5. Ainsi, le New York Times a censuré un télégramme dans lequel il était écrit que des millions de dollars avaient été distribués à des Libyens influents par l'intermédiaire de compagnies pétrolières et de gaz opérant en Libye. Le télégramme ne mentionnait pas le nom d'une seule de ces compagnies, mais le New York Times a choisi de supprimer les mots « compagnies de services pétroliers »6. Le cas le plus flagrant concerne indiscutablement l'exploitation par le New York Times d'un télégramme de soixante-deux pages sur le programme de missiles nord-coréen et leur possible vente aux Iraniens. Le New York Times a extrait deux paragraphes de ce télégramme pour tenter de démontrer que l'Iran disposait de missiles pouvant atteindre l'Europe, alors que d'autres passages du même télégramme disaient le contraire7.

Quant au Guardian, il a caviardé un télégramme au sujet de Ioulia Timochenko, l'ex-Premier ministre ukrainienne, qui évoquait la fortune qu'elle aurait dissimulée à Londres8. Le Guardian a également sucré des commentaires sur la corruption généralisée des élites kazakhes – alors même qu'aucun nom n'était cité – et d'autres remarques selon lesquelles ENI, l'entreprise pétrolière nationale italienne opérant au Kazakhstan, ainsi que British Gas, étaient corrompues9. En gros, le Guardian caviardait les télégrammes lorsqu'une personne fortunée était accusée de quelque chose, sauf si le Guardian avait ses propres raisons pour s'en prendre à cette personne10. Donc, par exemple, dans un télégramme sur le crime organisé en Bulgarie, il était question d'un Russe. La présentation du Guardian donnait l'impression qu'il s'agissait d'un personnage central, alors qu'il faisait partie d'une longue liste d'organisations et d'individus associés au crime organisé bulgare11. Der Spiegel a censuré un paragraphe sur Merkel – son manque d'intérêt pour les questions de droits de l'homme, et d'autres considérations d'ordre purement politique au sujet de Merkel12. Les exemples abondent13.

ANDY : Notre conception de la liberté d'informer et de la libre circulation des informations est en un sens un concept radicalement nouveau si l'on considère les choses à l'échelle planétaire. Je dirais que pas grand-chose ne distingue l'Europe d'autres pays. Certains pays ont un cadre démocratique, ce qui veut dire que l'on peut lire et comprendre et même combattre légalement la structure de la censure, mais pas qu'elle n'existe pas. En Arabie saoudite ou en Chine, si vous essayez de mener ce type de combat, cela se passera beaucoup moins bien pour vous.

JULIAN : Mon expérience ne cesse de me démontrer que les pays occidentaux sont simplement bien plus sophistiqués au niveau de la désinformation et de la dissimulation de la réalité. Il y a une multiplicité de niveaux qui permettent de nier l'existence de la censure. La censure est comme une pyramide enfouie. Seule la pointe émerge du sable, et pour cause. Seule la pointe est publique – procès en diffamation, assassinats de journalistes, caméras saisies par les militaires et ainsi de suite –, il s'agit de la censure publiquement reconnue. Mais ce n'est qu'une infime partie de l'ensemble. Sous la pointe, la couche suivante est celle de toutes ces personnes qui préfèrent ne pas être vues, qui pratiquent l'autocensure pour éviter de se retrouver sur la pointe. La couche suivante contient toutes les formes d'incitations économiques et d'aides que l'on accorde aux gens pour parler de telle chose plutôt que de telle autre. Plus bas encore se trouve la couche de l'économie brute – les sujets sur lesquels il est économique d'écrire, même si vous ne tenez pas compte des facteurs économiques qui proviennent des niveaux supérieurs de la pyramide. La couche suivante, ce sont les préjugés des lecteurs avec un faible niveau d'éducation, qui sont donc des cibles faciles pour la désinformation, et à qui l'on ne peut même pas expliquer des choses sophistiquées. La dernière couche est celle de la distribution – certaines personnes, par exemple, n'ont tout simplement pas accès à de l'information dans une langue donnée. C'est ça, la pyramide de la censure. Quand il censure les télégrammes du Cablegate, le Guardian s'inscrit dans le deuxième niveau.

Cette censure est facile à nier, soit parce qu'elle se fait à l'abri des regards, soit parce que aucune instruction n'est jamais donnée de censurer telle ou telle affirmation. Il est rare qu'on dise à un journaliste : « N'écris rien là-dessus » ou : « Ne parle pas de ça. » Ils savent très bien ce qu'ils sont censés faire et ne pas faire sans qu'on ait besoin de leur dire parce qu'ils comprennent les intérêts de ceux qu'ils souhaitent satisfaire ou dont ils souhaitent se rapprocher. Si vous vous conduisez bien, on vous donnera une petite tape sur la tête et on vous récompensera, sinon, ça sera moins sympa. C'est aussi simple que ça. J'aime bien l'exemple de la censure soviétique, cette censure dont la propagande faisait si bien ses choux gras en Occident – les chaussures à clous qui viennent arrêter les journalistes chez eux en pleine nuit, etc. En fait, elle a subi un décalage horaire de douze heures, c'est tout. À présent, on attend que le jour soit levé et on prend la maison du journaliste, une fois qu'il est tombé en disgrâce et qu'il ne peut plus payer ses dettes. On ne vient plus prendre le journaliste dans sa maison, c'est sa maison qu'on vient lui prendre. Les sociétés occidentales se sont fait une spécialité du blanchiment de la censure en structurant les affaires des puissants de sorte qu'aucune voix qui perce dans le débat public ne puisse réellement modifier les relations de pouvoir parce que ces relations sont camouflées sous de multiples couches de complexité et de secrets.

ANDY : Les pédo-nazis de Jérémie.

JACOB : Nous voici revenus aux pédo-nazis.

JÉRÉMIE : Deux Cavaliers de l'Infocalypse pour le prix d'un.

ANDY : Les pédo-nazis résument assez bien les arguments allemands, voire une partie des arguments européens en faveur de la censure. En raison de son passé, l'Allemagne ne veut pas de contenus haineux sur Internet, et bien évidemment si vous dites aux gens que c'est à cause des pédophiles qu'il faut limiter l'accès à Internet, vous pourrez faire tout ce que vous voudrez. Il existe un do-

cument de travail interne de la Commission européenne sur la rétention des données qui soutenait que si « on parle davantage de la pornographie infantile, alors les gens seront pour14 ».

JULIAN : On pourrait parler un peu plus de ça, de l'idée que pour censurer une chose donnée, disons la pornographie infantile, pour interdire aux gens d'y avoir accès, il faut surveiller tout le monde. On doit donc mettre sur pied l'infrastructure nécessaire, un système global d'espionnage et de censure dans le but de censurer une seule chose.

ANDY : Tout est dans les détails du mécanisme, le prétendu système de précensure allemand te fait obligation de désigner une personne légalement responsable. Donc, en gros, si tu publies quelque chose, que ce soit sur un bout de papier ou sur Internet, sans dire qui est légalement responsable, tu violes déjà la loi. Il y a donc une assignation de responsabilité, et si quelqu'un viole la loi en diffusant par exemple de la pornographie infantile ou des discours de haine, on pourra dire : « OK, voyons voir où se trouve ce gars, mettons la main sur lui et enlevons tous ces trucs du Net. »

JULIAN : C'est-à-dire que l'on censure l'éditeur au lieu de censurer le lecteur.

ANDY : Exactement. En l'occurrence il s'agit de surveiller des choses précises. Je pourrais être d'accord pour dire que tout ne peut pas être mis à disposition à tout instant, parce que s'il s'agit d'incitations à la haine, il y a parfois l'adresse personnelle de gens, et ainsi de suite, et cela pourrait aboutir à des situations avec lesquelles je ne suis pas d'accord.

JULIAN : Andy, c'est tellement allemand tout ça. Pour faire ça, pour décider ce qui est acceptable et ce qui ne l'est pas, il faut un comité, il faut nommer des gens à ce comité, il faut un processus de nominations à ce comité...

ANDY : Oui, oui, il y a toute cette merde. Les victimes de la Seconde Guerre mondiale tuées par les Allemands – tout ce qu'ont fait les nazis, tous les biens qu'ils ont saisis, pour lesquels ils ont donné

des reçus, établi une liste. Ce n'étaient que des gestes bureaucratiques. On peut dire avec raison que les Allemands ont tué beaucoup de monde de manière totalement injustifiée, mais ils l'ont fait d'une manière totalement bureaucratique. C'est ça, l'Allemagne.

JULIAN : À partir du moment où quelqu'un décide de ce qui sera censuré et de ce qui ne le sera pas, il se produit deux choses. Il faut d'abord mettre sur pied une architecture technique pour effectuer la censure. Il faut une machinerie nationale pour censurer de manière efficace. Ensuite, il faut un comité et une bureaucratie chargés de la censure. Ce comité sera forcément secret, puisqu'il n'a aucune utilité s'il ne l'est pas, et il y aura donc une justice secrète.

ANDY : Vous savez quoi ? Nous avons un bon principe en Allemagne.

JACOB : Un seul ?

ANDY : C'est le principe selon lequel une loi qui ne peut être appliquée de manière réaliste n'a pas lieu d'exister. Si une loi ne tient pas debout, par exemple si vous décidez d'interdire les moulins à vent ou quelque chose dans le genre, alors on dit : « Hé, laisse tomber. » Nous qui sommes réunis ici, nous puisons notre inspiration dans l'Internet des débuts, la libre circulation de l'information, « libre » voulant dire non limité, non bloqué, non censuré, non filtré. Donc, si nous appliquons cette idée de la libre circulation de l'information au monde entier – et c'est de fait ce qui se passe –, il devient clair que cela influe les gouvernements, la manière dont le pouvoir est utilisé, dont la censure est mise en œuvre, qu'il s'agisse de précensure, de post-censure, ou de n'importe quoi d'autre. Nous savons bien que cela peut donner naissance à des conflits compliqués. La question est : quelle est notre conception d'un gouvernement futur, ou d'une organisation postgouvernementale, WikiLeaks étant peut-être la première ou une des premières organisations postgouvernementales. Je ne suis pas convaincu que les gouvernements soient la meilleure réponse à tous les problèmes de la planète, comme les questions environnementales.

JULIAN : Les gouvernements ne le savent pas bien non plus, ils ne sont pas sûrs de la ligne de démarcation entre ce qui est gouvernemental et ce qui ne l'est pas. Ça s'est brouillé. Les gouvernements occupent l'espace mais, sur Internet, WikiLeaks occupe aussi une partie de l'espace. L'espace Internet fait partie de l'espace réel, mais la complexité du rapport entre l'objet intégré et la partie intégrante signifie qu'il n'est pas facile pour la partie intégrante de savoir si l'objet intégré fait même partie d'elle. C'est pour cela que nous concevons le cyberespace comme une sorte de royaume ayant une existence quelque part : c'est parce qu'il combine absence de finalité, complexité et universalité. Quand vous lisez un fichier quelque part sur Internet, peu importe l'endroit dans l'espace ou le temps où il se trouve – c'est ça, son universalité. Donc, puisque nous sommes une organisation qui vit dans le cyberespace, passée maître dans l'art de manier la relocalisation de ses informations dans le substrat physique sous-jacent, libre de tout contrôle géographique, nous sommes peut-être une organisation postgouvernementale.

Je ne vais pas pousser cette analogie plus loin, parce que je suis aux arrêts domiciliaires. La force de

coercition des États s'applique à nos associés dès que leur nom est mis sur la place publique. La presse aime nous présenter comme un média sans État, et elle a raison d'insister sur l'importance de l'absence d'État. Je l'ai toujours dit : « Que croyez-vous donc qu'est News Corp ? Ce n'est qu'une grande multinationale. » La structure de News Corp fait que l'on peut atteindre ses composants essentiels, et c'est la raison pour laquelle ils ont tellement d'ennuis en ce moment au Royaume-Uni, avec le scandale des écoutes téléphoniques, et c'est pour la même raison qu'ils se mettent en quatre pour faire de la lèche à l'establishment américain. Mais si une organisation a pour principale ressource ses propres informations, et qu'elle utilise la cryptographie, alors elle peut être transnationale d'une manière assez difficile à contrecarrer. Il y a une raison au blocus financier qui nous a été imposé : les autres aspects de notre organisation sont plus difficiles à bloquer15.

JACOB : Pour parler en termes utopiques, remontons un peu dans le temps. Tu t'interroges sur le harcèlement dont j'ai été l'objet, tu t'interroges sur la censure dans les pays occidentaux, et plus tôt j'ai évoqué le programme d'assassinats ciblés d'Obama, qui est censé être légal du fait qu'il obéit à un processus, lequel compte donc en tant que processus légitime.

JULIAN : Il s'agit d'un processus secret, en fait.

JACOB : On peut faire remonter ça à John Gilmore. L'une des procédures judiciaires intentées par Gilmore visant son droit à voyager aux États-Unis sans faire état de son identité a débouché sur la déclaration suivante du tribunal : « Écoutez, on va consulter la loi, qui est secrète. On va la lire pour voir si, selon cette loi secrète, vous avez le droit de faire ce que vous dites avoir le droit de faire. » Et ils ont lu la loi secrète, et en fait le droit était de son côté, parce que la loi secrète ne pouvait s'appliquer à lui. Il n'y a pas eu moyen de savoir ce que contenait cette loi secrète, et, par la suite, après sa victoire devant le tribunal, ils ont modifié les règlements de l'US Transportation Security Administration et du Department of Homeland Security, parce que la loi secrète, en l'état, n'était pas assez contraignante16.

JULIAN : Donc, ils l'ont rendue plus contraignante ?

JACOB : Oui, en permettant à la bureaucratie de légiférer. L'important, c'est que tout est lié, les assassinats ciblés, le harcèlement des individus aux frontières, la censure qui existe en ligne, la censure que les grandes entreprises mettent en œuvre pour satisfaire aux demandes du gouvernement ou d'autres grandes entreprises. Et le fond de l'histoire, c'est que cela se produit là où, précisément, l'État dispose d'un excès de pouvoir. Le pouvoir y est en quelque sorte concentré, et cela attire des gens qui en abusent ou qui encouragent pour qu'il en soit fait usage. Il existe peut-être des cas légitimes, mais une chose est sûre : le monde serait meilleur si toute cette centralisation n'existait pas, si ces tendances autoritaires n'existaient pas.

L'Occident n'a aucun statut privilégié concernant tout cela, parce que le fait d'avoir un « tsar » de la cybersécurité n'est pas très différent que d'avoir un « tsar » des forces de sécurité comme celui d'une certaine nation il y a un demi-siècle. Nous mettons en place le même type de structures de

contrôle autoritaires, des gens seront forcément tentés d'en abuser, et la seule raison pour laquelle nous aimons croire qu'il en va autrement chez nous, c'est qu'il existe un continuum de la gouvernance qui va de l'autoritarisme au libertarisme. Je n'emploie pas le terme au sens américain, mais au sens où, dans ce continuum, les États-Unis sont très loin de l'Union soviétique à de nombreux égards, mais plus proches d'elle que, disons, la communauté autonome de Christiania, au centre de Copenhague17. Et encore plus loin, je pense, d'une société utopique que l'on pourrait fonder sur Mars. Si l'on fondait une colonie sur Mars, on voudrait qu'elle soit le plus loin possible du totalitarisme et de l'autoritarisme. Si l'on n'y prend pas garde, on se retrouve rapidement avec des problèmes.

JÉRÉMIE : Là encore, toutes ces questions sont liées. Quand on parle de la concentration du pouvoir, on parle à nouveau de l'architecture. Et quand on parle de la censure sur Internet, il s'agit de la centralisation du pouvoir de décider ce que les gens peuvent ou ne peuvent pas voir, de savoir si toute censure gouvernementale ou privée est un excès de pouvoir. Prenons un exemple : notre site laquadrature.net a été censuré par Orange UK au Royaume-Uni durant plusieurs semaines. Il faisait partie d'une liste de sites qu'Orange a interdit aux moins de dix-huit ans. Peut-être avions-nous utilisé les mots « pornographie infantile » au moment où nous nous opposions à la législation sur ce sujet, ou peut-être nous avaient-ils pris en grippe parce que nous nous opposons à leur politique contraire à la neutralité du Net, et que nous défendons une loi visant à leur interdire de faire un tri parmi les communications de leurs utilisateurs18. On ne le saura sans doute jamais. Mais cet acteur privé, en tant que prestataire de services, s'est arrogé le droit de priver les gens de leur libre accès à des informations sur Internet. Pour moi, cela représente un risque majeur, qui dépasse de loin le problème du pouvoir que nous accordons à Orange, ou au gouvernement chinois, ou à qui que ce soit d'autre.

JACOB : Une petite clarification, quand tu dis « privé », s'agissant du Royaume-Uni, tu veux dire qu'ils sont propriétaires des lignes, de toutes les connexions par fibre optique et de tout, absolument tout, ou bien utilisent-ils des ressources publiques ? Comment sont gérées les ondes hertziennes ? L'État n'est pas du tout impliqué ? Aucune obligation d'entretien ?

JÉRÉMIE : C'est un système de licences. Qu'il s'agisse de l'État ou d'une entreprise, ils sont en train de transformer l'architecture d'Internet, qui cesse d'être un réseau universel unique pour devenir un système balkanisé de petits sous-réseaux. Mais les questions dont nous discutons depuis le début sont des questions globales, qu'il s'agisse du détraquement du système financier, de la corruption, de la géopolitique ou de l'environnement. Il s'agit de problèmes globaux auxquels l'humanité doit faire face aujourd'hui, et nous disposons d'un outil global qui permet une meilleure communication, un meilleur partage des connaissances, une meilleure participation aux processus politiques et démocratiques. Je pense qu'un Internet global et universel est le seul outil permettant de répondre à ces questions globales, et que c'est la raison pour laquelle ce combat pour un Internet libre est un combat fondamental, et que notre responsabilité à tous est de le mener.

ANDY : Je suis complètement d'accord, il faut non seulement faire en sorte qu'Internet soit compris comme un réseau universel dans lequel l'information circule librement, il faut non seulement que nous définissions cela de manière très précise, mais nous devons aussi dénoncer les

entreprises et les fournisseurs d'accès qui proposent quelque chose qu'ils appellent Internet mais qui n'a rien à voir avec Internet. Cela dit, je pense que nous n'avons pas répondu à la question fondamentale qui se cache derrière cette histoire de filtrage. Je vais vous donner un exemple de ce que je veux dire. Il y a quelques années, une dizaine d'années environ, nous avons mené une campagne contre un logiciel de prétendu « filtrage intelligent » que Siemens proposait en Allemagne. Siemens est l'une de nos plus importantes entreprises de télécom, et ils développent aussi des logiciels pour le renseignement. Ils ont vendu ce système de filtrage à des sociétés, de sorte que, par exemple, les employés se voyaient interdire l'accès au site de leur syndicat s'ils souhaitaient s'informer sur leurs droits et ainsi de suite. Ils ont également bloqué le site du Chaos Computer Club, ce qui nous a pas mal énervés. Ils nous ont signalés comme étant du « contenu criminel » ou quelque chose dans le genre, et on les a traînés en justice. Pour marquer le coup, on a décidé d'organiser une protestation pendant un salon auquel participait Siemens. On a entouré leur stand et on a filtré les gens qui entraient et sortaient. L'ironie de l'histoire, c'est qu'on l'avait annoncé sur notre site pour attirer le plus de monde possible, mais les gens de chez Siemens n'étaient au courant de rien puisque leur propre système de filtrage leur interdisait d'accéder à notre site.

JULIAN : Le Pentagone a mis en place un système de filtrage qui bloquait tout mail envoyé au Pentagone contenant le mot clé « WikiLeaks ». Donc, quand le procureur militaire qui instruisait l'affaire Bradley Manning envoyait des mails au sujet de WikiLeaks à des personnes extérieures, il ne recevait jamais leurs réponses parce qu'elles contenaient le mot « WikiLeaks »19 ! L'État sécuritaire va peut-être réussir à se dévorer lui-même.

ANDY : Ce qui nous ramène à une question plutôt basique : l'information à effet négatif existe-t-elle vraiment ? Du point de vue de la société, voulons-nous vraiment d'un Internet censuré parce que c'est « mieux pour la société » ? Et même dans le cas de la pornographie infantile, on pourrait dire : « Hé, minute, cette histoire de pornographie infantile est révélatrice d'un problème, celui de la pédophilie, mais pour combattre le problème, il faut le connaître. »

JACOB : Et donc pouvoir disposer des preuves de l'activité criminelle en question.

JULIAN : Ça conduit surtout à la formation d'un lobby.

ANDY : Ça, c'est l'approche radicale, mais s'il s'agit de nazis par exemple, il faut quand même être capable de dire de quoi on parle. Les gens qui ont une famille vont se demander : « C'est peut-être bien pour la société de filtrer les contenus nocifs pour ne garder que ce qui est bien, mais cela ne nous empêchera-t-il pas de percevoir les problèmes, de les gérer, de s'en occuper, et de les régler ? »

JÉRÉMIE : Je pense que la censure n'est jamais la solution. S'agissant de pornographie infantile, on ne devrait même pas utiliser le mot « pornographie » – ce sont en fait des images de scènes de

crime dans des affaires d'abus sexuels sur enfants. Ce qu'on peut faire, c'est aller voir du côté des serveurs, déconnecter les serveurs, identifier les gens qui ont déposé ces contenus, identifier ceux qui ont commis ces abus sur ces enfants. Et, dès qu'il s'agit d'un réseau de personnes, un réseau commercial et ainsi de suite, il faut les arrêter. Mais quand on adopte des lois comme celle qui existe en France, où une autorité administrative dépendant du ministère de l'Intérieur peut bloquer des sites, les services d'enquête sont moins enclins à rechercher les responsables. Ils se contentent de dire : « Oh, nous avons interdit l'accès. » C'est comme si on mettait la main devant les yeux de quelqu'un qui regarde le problème et qu'on pensait l'avoir résolu. Donc, de ce point de vue, je crois qu'il suffit de dire : nous sommes tous d'accord pour faire disparaître ces images d'Internet.

JACOB : Je suis désolé, mais je ne tiens plus. C'est vraiment dingue ce que tu viens de dire, ça me donne envie de gerber, parce que tu dis, en gros : « Je vais utiliser ma position de pouvoir pour affirmer mon autorité sur d'autres personnes, je vais effacer l'histoire. » Vous allez peut-être me trouver extrémiste dans le cas présent – et dans bien d'autres cas aussi, j'en suis sûr –, mais je vais aller au bout de mon raisonnement. Il s'agit en fait d'une situation où l'on ne se rend pas service en effaçant l'histoire. Donc, grâce à Internet, on sait qu'il y a une épidémie d'abus sexuels sur des enfants dans notre société. C'est ça, la leçon de cette histoire de pédophilie sur Internet – j'ai plus envie d'appeler ça de l'exploitation sexuelle d'enfants. C'est une imposture de chercher à se voiler la face en effaçant les traces, parce qu'elles nous renseignent sur la société dans son ensemble. Par exemple, cela nous permet d'apprendre – et je pense qu'après la phrase qui suit je ne ferai pas une carrière politique, mais je préfère être clair – qui fait cela, et qui sont les victimes. On ne peut pas se contenter d'ignorer le problème. Il faut commencer par chercher la cause de tout cela, à savoir les gens qui exploitent les enfants. Ironiquement, des logiciels de surveillance pourraient être utiles, pour identifier les visages des gens et en fouillant dans les métadonnées des images. Si on efface tout cela, si on décide de vivre dans un monde où il est possible d'effacer certaines choses et pas d'autres, si l'on crée des organismes administratifs pour la censure et le maintien de l'ordre, on s'engage sur une pente savonneuse qui, comme nous l'avons vu, permettra de passer ensuite directement aux questions de copyright, et à bien d'autres domaines.

Le fait qu'il s'agisse d'une cause digne d'être défendue ne justifie pas le choix de la facilité. Peut-être faudrait-il, en fait, s'efforcer de résoudre les crimes, peut-être devrait-on essayer d'aider les victimes, même si ce type d'aide comporte un coût. Peut-être que, au lieu d'ignorer le problème, on ferait mieux de reconnaître que c'est un problème de la société dans son ensemble, et qu'il se manifeste d'une certaine manière sur Internet.

Prenons un autre exemple : lorsque Polaroid a commercialisé ses appareils à développement instantané, certains s'en sont servis pour prendre des photos d'abus sexuels. Mais personne n'a jamais prétendu détruire le médium. L'important, c'est d'obtenir des preuves matérielles permettant de poursuivre en justice les crimes qui ont été révélés par ce médium. Le but n'est pas d'affaiblir le médium, ce n'est pas de pénaliser toute la société à cause de ce problème. Parlons des pédophiles, d'accord, mais parlons aussi de la police. La police, dans toutes sortes de pays à travers le monde, maltraite des gens. Il y a probablement plus de flics pourris sur Internet que de pédophiles.

JULIAN : C'est fort probable.

JACOB : Disons qu'il y a n policiers dans le monde et que x de ces n policiers sont coupables de

fautes déontologiques – en général des actes violents. Il suffit de voir comment a été réprimé le mouvement Occupy pour s'en persuader. Doit-on censurer Internet parce que certains flics sont mauvais ? Doit-on limiter sévèrement la capacité de la police à faire du bon travail ?

JULIAN : Bon, il y a la question de la revictimisation, qui a lieu lorsque l'enfant, par la suite, ou une fois devenu adulte, ou ses connaissances revoient les images des abus dont il a été victime.

JACOB : Tant que ces flics sont en ligne, je me sentirai revictimisé.

JULIAN : On pourrait dire que le fait de te revoir te faire matraquer par un flic est une revictimisation. Mais je pense que la protection de l'intégrité de l'histoire de ce qui s'est effectivement passé dans notre monde prime sur tout ; la revictimisation existe bien, mais la mise en place d'un système de censure capable de faire disparaître des pans entiers de notre histoire signifie qu'on ne pourra pas répondre au problème parce qu'on ne pourra plus le voir. Dans les années 1990, j'ai travaillé en tant que consultant sur les questions d'Internet auprès des services de police australiens spécialisés dans la lutte contre l'exploitation sexuelle des enfants, la Victorian Child Exploitation Unit. Ces flics ne voyaient pas d'un bon œil les systèmes de filtrage, parce que lorsque les gens ne peuvent plus voir qu'il y a de la pédophilie sur Internet, le lobby qui permet à ces flics de trouver des financements s'étiole.

JÉRÉMIE : Je pense que nous serons tous d'accord pour dire que ce qui compte, au fond, c'est la responsabilité individuelle des gens qui produisent ces contenus, les photos pédophiles et autres choses dans le genre, c'est ça ce qui compte vraiment, et c'est là-dessus que les flics doivent se concentrer.

JACOB : Non, nous ne sommes pas tous d'accord. Ce n'est pas ce que j'ai dit.

JULIAN : En fait, Jérémie parle de produire, pas de publier, il y a une différence.

JACOB : Mais la production du contenu n'est pas non plus la question, en fait. Petite clarification : si tu as molesté un enfant et qu'Andy a pris une photo à titre de preuve, je ne pense pas qu'Andy doive être poursuivi.

JÉRÉMIE : Je ne suis pas d'accord, ils sont tous les deux responsables. Allez, il s'agit au moins de complicité.

ANDY : Certaines personnes abusent quand même des enfants pour produire les photos, n'est-ce pas ?

JACOB : Bien évidemment.

ANDY : La question comporte donc un aspect financier, également.

JACOB : Je suis tout à fait d'accord, je fais une distinction ici : si le contenu lui-même est une trace historique de la preuve matérielle d'un crime, c'est la preuve d'un crime très sérieux, et même en tenant compte de l'aspect revictimisation, la question centrale reste celle de la victimisation d'origine, qu'il y ait des photos ou non.

JÉRÉMIE : Bien sûr, c'est ce que je pense aussi.

JACOB : L'existence ou non de photos est presque hors de propos. Quand photos il y a, il faut se rappeler que le but recherché est de mettre un terme aux abus. Pour cela, il faut faire en sorte que des preuves matérielles soient disponibles et que les gens disposant des outils appropriés soient motivés pour résoudre ces crimes. Je pense que ça, c'est extrêmement important, et les gens le perdent de vue parce que la facilité, c'est de faire comme si tout cela n'existait pas, de chercher à l'interdire, et de dire ensuite qu'on a mis fin aux abus, alors que ce n'est pas le cas.

ANDY : Le problème, c'est qu'en ce moment beaucoup de gens préfèrent la solution de facilité parce qu'il est très déplaisant de regarder en face ce qui se passe dans notre société. Je crois qu'on a une chance de s'attaquer à un problème politique dès lors qu'on n'essaie pas de mettre en place des mesures qui ignorent le problème ou qui le dissimulent. C'est peut-être ça, la cyberpolitique. Mais la question, c'est aussi la manière dont la société règle ses problèmes, et je doute fortement que l'information nocive en soi existe réellement. C'est lié au filtrage, bien sûr, et il est vrai que je ne tiens pas à voir toutes les images qui sont disponibles sur Internet. Certaines d'entre elles me troublent, me dérangent, mais cela m'arrive également au magasin vidéo du coin, avec certains films, des fictions, que je trouve déplaisants. Donc, la question est : suis-je capable de choisir ce que je regarde, ce qui m'intéresse, ce que je lis ? C'est ça la philosophie du filtrage. Wau Holland, le fondateur du Chaos Computer Club, a dit quelque chose de très pertinent sur le sujet : « Le filtrage doit être à la charge de l'utilisateur final, au niveau du matériel final de l'utilisateur final20. »

JULIAN : Donc, le filtrage devrait incomber aux gens qui recoivent l'information.

ANDY : C’est ici que ça doit se passer. Pointant un doigt sur sa tête : Ici !

JULIAN : Dans notre cerveau.

ANDY : C’est ça, « le matériel final de l’utilisateur final », c’est ce truc que vous avez entre les oreilles. C’est là que doit intervenir le filtrage, et le gouvernement n’a rien à y faire. Personne ne vous oblige à voir ce que vous ne voulez pas voir, on filtre suffisamment de choses comme ça, de nos jours.

1. Pour plus de détails sur le harcèlement de Jacob et d’autres individus associés à WikiLeaks, voir le chapitre « À propos des diverses tentatives de persécution de WikiLeaks et des individus qui y sont associés ».

2. Isaac Mao est un blogueur, concepteur de logiciels et investisseur-risque chinois. Il est l’un des cofondateurs de CNBlog.org et membre du conseil d’administration du projet Tor.

3. Voir la page WikiLeaks sur Nadhmi Auchi : http://wikileaks.org/wiki/ Nadhmi_Auchi (lien vérifié le 24 octobre 2012).

4. On peut consulter les articles WikiLeaks ici : http://wikileaks.org/wiki/Eight_stories_on_Obama_linked_billionaire_Nadhmi_Auchi_censored_from_the_Guardian, _Observer,_Telegraph_and_New_Statesman (lien vérifié le 24 octobre 2012).

5. En comparant les télégrammes complets et censurés sur les sites et http://cablegatesearch.net, on obtiendra une version très précise des coupes opérées par les partenaires de WikiLeaks.

6. « Qaddafi’s Son Is Bisexual and Other Things the New York Times Doesn’t Want You to Know », Gawker, 16 septembre 2011 : http://gawker.com/5840809/qaddafis-son-is-bisexual-and-other-things-the-new-york-times-doesnt- want-you-to-know-about. L’exemple en question renvoie au télégramme n° 06TRIPOLI198, WikiLeaks : https://wikileaks.org/cable/2006/05/06TRIPOLI198.html. On peut visualiser les coupes sur le site Cablegatesearch qui en fait apparaître l’historique avec les parties omises surlignées en rose : http://www.cablegatesearch.net/cable.php?id=06TRIPOLI198&version=1291757400 (tous les liens ont été vérifiés le 22 octobre 2012).

7. Pour l'original, voir télégramme n° 10STATE 17263, WikiLeaks : http://wikileaks.org/cable/2010/02/ 10STATE17263.html. Pour l'article du New York Times voir « Iran Fortifies Its Arsenal With the Aid of North Korea », New York Times, 29 novembre 2010 : http://www.nytimes.com/2010/11/29/world/middleeast/29 missiles.html?_r=0.

Le même télégramme a aussi été utilisé par David Leigh du Guardian pour son article : « WikiLeaks cables expose Pakistan nuclear fears », Guardian, 30 novembre 2010 : http://www.guardian.co.uk/world/2010/nov/30/ wikileaks-cables-pakistan-nuclear-fears. La version censurée publiée par le Guardian ne donnait pas la référence du document et le réduisait à deux paragraphes sur le Pakistan. « US embassy cables : XXXXXXXXXXXX », Guardian, 30 novembre 2010 : http://www.guardian.co.uk/world/us-embassy-cables-documents/250573.

L'étendue des coupes peut être visualisée sur le site Cablegatesearch qui fait apparaître l'historique des révisions et la coupe, surlignée en rose, de la quasi-totalité du télégramme : http://www.cablegatesearch.net/cable.php?id=10STATE17263&version=1291486260 (tous les liens ont été vérifiés le 22 octobre 2012).

8. Voir le télégramme original n° 08KYIV2414 sur WikiLeaks : http://wikileaks.org/cable/2008/12/08 KYIV2414.html. Pour la version coupée du Guardian voir « US embassy cables: Gas supplies linked to Russian mafia », 1er décembre 2010 : http://www.guardian.co.uk/world/us-embassy-cables-documents/182121? INTCMP= SRCH. Les coupes peuvent être visualisées sur le site Cablegatesearch, qui permet de voir l'historique des révisions et les coupes surlignées en rose : http://www.cablegatesearch.net/cable.php? id=08KYIV2414&version= 1291255260 (tous les liens ont été vérifiés le 22 octobre 2012).

9. Voir le télégramme original n° ID 10ASTANA72 sur WikiLeaks :

http://wikileaks.org/cable/2010/01/10ASTANA72.html.

Pour la version coupée parue dans le Guardian voir « US embassy cables: Kazakhstan – the big four », Guardian, 29 novembre 2010 : http://www.guardian.co.uk/world/us-embassy-cables-documents/245167?INTCMP=SRCH.

Les coupes peuvent être visualisées sur le site Cablegatesearch, qui permet de voir l'historique des révisions et les coupes surlignées en rose : http://www.cablegatesearch.net/cable.php? id=10ASTANA72&version= 1291113360 (tous les liens ont été vérifiés le 22 octobre 2012).

10. Voir, par exemple, le télégramme n° 09TRIPOLI413 au sujet des compagnies pétrolières occidentales opérant en Libye. La représentation visuelle des coupes sur le site Cablegatesearch, avec les coupes du Guardian surlignées en rose, montre que le Guardian a enlevé les noms de toutes ces sociétés et de leurs dirigeants, exception faite de la compagnie russe Gazprom. Même si le contenu du télégramme n'incrimine pas trop gravement les compagnies occidentales, les coupes sont sophistiquées et le tableau qui se dégage de la version non expurgée est assez différent : http://www.cablegatesearch.net/cable.php?id=09 TRIPOLI413&ver-sion=1296509820 (lien vérifié le 22 octobre 2012).

11. Dans cet exemple, le télégramme original contenait 5 226 mots. La version expurgée publiée par

le Guardian n'en contenait plus que 1 406. Pour le télégramme original, voir télégramme n° 05SOFIA1207 sur WikiLeaks : http://wikileaks.org/cable/2005/07/05SOFIA1207.html.

Pour la version expurgée du Guardian voir « US embassy cables: Organised crime in Bulgaria », 1er décembre 2010 : http://www.guardian.co.uk/world/us-embassy-cables-documents/36013. Pour l'article du Guardian basé sur le télégramme voir « WikiLeaks cables: Russian government "using mafia for its dirty work" », Guardian, 1er décembre 2010 : hhttp://www.guardian.co.uk/world/2010/dec/01/wikileaks-cable-spain-russian-mafia.

On peut visualiser l'étendue des coupes sur le site Cablegatesearch qui présente l'historique des coupes avec les parties expurgées surlignées en rose : http://www.cablegatesearch.net/cable.php?id=05SOFIA1207&version= 1291757400. Cet exemple bulgare a été analysé par le partenaire bulgare de WikiLeaks, Bivol, dans « Unedited cable from Sofia shows the total invasion of the state by organized crime (Update : Cable Comparison) », WL Central, 18 mars 2011 : http://wlcentral.org/node/1480. Voir en outre, « The Guardian: Redacting, censoring or lying ? », WL Central, 19 mars 2012 : http://wlcentral.org/node/1490. Voir aussi sous les articles de WL Central le commentaire du journaliste du Guardian David Leigh et les réponses (tous les liens ont été vérifiés le 22 octobre 2012).

12. Ceci renvoie au télégramme n° 09BERLIN1108. Les coupes peuvent être visualisées sur le site Cablegatesearch, qui permet de voir l'historique des révisions et les coupes surlignées en rose : http://www.cablegatesearch.net/cable.php?id=09BERLIN1108&version= 1291380660 (lien vérifié le 22 octobre 2012).

13. Pour d'autres exemples, voir le site cabledrum : www.cabledrum.net/pages/censorship.php.

14. « Interception des télécommunications. La Présidence a fourni des informations sur l'état des choses... Elle rappelle la couverture négative que cette question a reçue dans les médias... Dans ce contexte, la Présidence a reconnu que les progrès dans ce domaine sont très lents. Plusieurs délégations ont exprimé des réserves quant à la préparation d'un communiqué de presse, faisant remarquer que ceci pouvait provoquer une réaction en chaîne et une nouvelle salve d'articles négatifs dans la presse. La Commission, tout en notant que sa position n'a pas changé, a informé les délégations qu'une possiblité pour sortir de l'impasse serait de suivre une stratégie semblable à celle qui a été mise en œuvre sur la question de la pornographie infantile sur Internet. Tout en reconnaissant qu'il s'agit d'un tout autre sujet, il y a aussi une dimension d'interception », Commission européenne, Groupe de travail sur la coopération policière, réunion sur l'interception des télécommunications, 13-14 octobre 1999. Le document est disponible dans son intégralité sur : http://www.quintessenz.at/doqs/000100002292/1999_10_13,Police%20 Cooperation%20Working %20Group%20mixed%20committee%20meeting.pdf (lien vérifié le 24 octobre 2012).

15. Voir le chapitre « À propos des diverses tentatives de persécution de WikiLeaks et des individus qui y sont associés ».

16. Jacob fait allusion au jugement « Gilmore vs Gonzales », 435 F.3d 1125 (9th Cir. 2006). John

Gilmore, un des cypherpunks originels, avait réussi à faire examiner son affaire par la Cour suprême pour obtenir la divulgation d'une loi secrète, une « directive de sécurité » limitant le droit des citoyens à voyager par avion sans pièce d'identité. Outre qu'il contestait la constitutionnalité de cette règle, Gilmore contestait le fait que la directive elle-même était secrète et ne pouvait être divulguée, alors que ses effets s'imposaient à tous les citoyens américains. La Cour avait consulté la directive secrète à huis clos et avait statué contre Gilmore. Toutefois, le contenu de cette loi n'a jamais été dévoilé pendant les débats. Voir « Gilmore vs Gonzales » sur PapersPlease.org : http://papersplease.org/gilmore/facts.html (lien vérifié le 22 octobre 2012).

17. Christiania est un quartier de Copenhague, au Danemark, qui a proclamé son autogouvernement. Il s'agit d'une ancienne caserne qui avait été occupée dans les années 1970 par une communauté anarcho-collectiviste. Elle a obtenu un statut légal unique au Danemark.

18. Le principe de « neutralité du Net » exige qu'il soit interdit aux FAI (par la loi, dans la version habituelle) de restreindre l'accès de leurs utilisateurs aux réseaux qui font partie d'Internet, y compris de restreindre l'accès à des contenus. Voir la page de l'Electronic Frontier Foundation sur la neutralité du Net : https://www.eff.org/issues/net-neutrality (lien vérifié le 24 octobre 2012).

19. « Blocking WikiLeaks emails trips up Bradley Manning prosecution », Politico, 15 mars 2012 : http://www.politico.com/blogs/under-the-radar/2012/03/blocking-wikileaks-emails-trips-up-bradley-manning-17573. html (lien vérifié le 21 octobre 2012).

20. Pour plus d'informations sur Wau Holland, voir le Wau Holland Stiftung : http://www.wauland.de.

Vie privée pour les faibles,

transparence pour les puissants

JULIAN : Il n'y a pas longtemps, j'ai parlé avec le président tunisien et je lui ai demandé ce qu'ils comptaient faire des archives des services secrets de Ben Ali – les archives de leur Stasi. Il m'a répondu que les services de renseignements restaient un problème, qu'ils étaient toujours dangereux, qu'il fallait les démanteler un à un, mais que les archives étaient très intéressantes. Selon lui, il vaut mieux qu'elles restent fermées pour des raisons de cohésion sociale, pour éviter une chasse aux sorcières. Andy, tu étais un jeune homme à l'époque de la chute de la RDA, tu peux nous parler de ton expérience ? Qu'est-ce que tu penses de l'ouverture de ce type d'archives ?

ANDY : L'Allemagne dispose de l'une des archives les plus complètes au monde d'un service de sécurité d'État. Tous les documents de la Staatssicherheit de la RDA, toutes les notes, tous les comptes-rendus, tous les manuels, toutes les procédures, tous les documents de formation, toutes les études internes – tout, en gros, est public. « En gros », ça veut dire que certains documents sont plus difficiles d'accès que d'autres, mais une grande partie est facilement disponible. Le gouvernement à mis sur pied un organisme chargé de la sauvegarde de ces archives, et tous les citoyens allemands peuvent obtenir la communication de leur dossier personnel.

JULIAN : L'organisme en question, le grand distributeur d'archives de la Stasi, c'est le BStU (Bundesbeauftragte für die Stasi-Unterlagen).

ANDY : Oui, et lorsque des journalistes souhaitent enquêter sur tel ou tel sujet, ils peuvent également soumettre des « demandes de recherches », qui sont en quelque sorte l'équivalent des demandes fondées sur le Freedom of Information Act aux États-Unis. Les archives contiennent beaucoup de livres, ainsi que toutes sortes de manuels de formation qui expliquent comment la Stasi agissait. Tout ça est très révélateur, très intéressant. C'est peut-être en demander trop aux Tunisiens qu'ils ouvrent totalement les archives des services de sécurité, le président lui-même doit probablement vouloir tenir compte de ce que contiennent son propre dossier, les dossiers de ses alliés et ainsi de suite. Les services de sécurité se moquent totalement du respect de la vie privée, et ils collectent toutes sortes d'informations sur votre vie sexuelle, vos communications, vos transferts d'argent, bref sur tout ce que vous avez fait, et tout le monde n'a pas forcément envie que tout soit étalé sur la place publique.

JULIAN : Tu as suivi ce qui se passe avec le service de sécurité intérieure égyptien, le Amn al-Dawla ? Des milliers de gens ont pris d'assaut leurs archives au moment où on essayait de les brûler, de les détruire, de tout jeter à la poubelle, et beaucoup d'entre elles se sont retrouvées étalées un peu partout. Pour 2 dollars, tu pouvais acheter un dossier au marché et le mettre en ligne. Ça n'a pas détruit la société égyptienne.

ANDY : Je ne dis pas que ça menace de détruire la société, je dis juste que je comprends les gens qui n'ont pas envie de voir leur dossier mis sur la place publique. Venant d'un pays où les services de sécurité ont surveillé tout le monde pendant quarante ans, où chaque fois que j'allais pisser, c'était enregistré quelque part, je trouve ça compréhensible.

JULIAN : Mais il faut quand même analyser le rapport coûts-bénéfices, non ? Pour moi, balance un jour, balance toujours.

ANDY : Peut-être, mais l'éthique du hacker, c'est quand même d'exploiter les données et les informations publiques et de protéger les données et les informations privées. J'estime que si on se bat pour le respect de la vie privée – et les raisons de le faire sont légion – on ne peut pas se réfugier

derrière une analyse comparée des avantages et des inconvénients dans ce cas précis. On doit faire le tri. On n'est pas obligé de tout rendre public.

JACOB : Mais les avantages du secret ne sont pas les mêmes pour tout le monde. Considérons ton argumentation sous un autre angle, elle me semble pécher sur un point : le fait que l'accès à certaines données soit restreint n'implique pas qu'elles sont privées. C'est tout simplement faux. Chez moi, par exemple, un million de personnes ont le droit d'accéder à ces données privées...

JULIAN : En fait, ils sont 4,3 millions...

JACOB : Comment peut-on soutenir que ces données sont privées ? Le problème est justement qu'elles ne sont pas à l'abri de tous les regards.

JULIAN : Le secret s'applique à Monsieur Tout-le-monde, mais pas aux puissants.

ANDY : Oui, tu as raison, mais de là à ouvrir en grand les archives...

JULIAN : Certains pays européens l'ont fait.

ANDY : Non, je pense que les archives n'ont été rendues totalement publiques dans aucun pays.

JULIAN : En Pologne, par exemple, ils sont allés plus loin qu'en Allemagne.

ANDY : Peut-être. Mais la face sombre de ce qu'on a fait en Allemagne, c'est qu'on a laissé des ex-officiers de la Stasi non seulement se charger des archives, mais aussi administrer une partie de ce qu'on appelle la « Nouvelle Allemagne », le territoire de l'ex-RDA. Il y a une histoire édifiante à ce propos : l'entreprise qui a remporté l'appel d'offres pour l'entretien du bâtiment où sont conservées les archives de la Stasi a été choisie pour la simple raison qu'elle proposait le meilleur prix. Il a fallu six ans à l'organisme chargé de la conservation des archives pour découvrir que cette société avait été créée par des anciens de la Stasi pour nettoyer leurs propres archives !

JÉRÉMIE : J'ai lu quelque chose là-dessus sur WikiLeaks. C'était incroyable1.

ANDY : WikiLeaks a publié un rapport sur cette question, et tu as raison de dire que dès lors que ces archives existent et se retrouvent entre les mains des mauvaises personnes, c'est difficile d'affirmer qu'elles sont de nature privée.

JULIAN : Essayons d'élargir la discussion. Internet a conduit à une explosion de l'information dont dispose le public, c'est tout simplement exceptionnel. Leur utilité éducative est extraordinaire. D'un autre côté, depuis les révélations de WikiLeaks les gens disent : « Bon, toutes ces informations gouvernementales ultraconfidentielles sont publiques à présent, les gouvernements ne peuvent plus rien garder secret. » Je pense que c'est des conneries. Pour moi, WikiLeaks dévoile l'ombre d'une ombre. Nous avons peut-être mis plus d'un million de mots à la disposition du public, mais cela ne fait que refléter l'immense explosion de la quantité de documents secrets aujourd'hui. En fait, certains groupes puissants disposent de quantités colossales d'informations secrètes à côté desquelles les données publiques font pâle figure. Les opérations de WikiLeaks ne concernent qu'un infime pourcentage de ce matériel secret. Si l'on considère, d'une part, les puissants qui sont au courant de la moindre transaction de carte de crédit au monde et, de l'autre, les gens ordinaires qui utilisent Google et lisent des blogs, peut-on parler d'un rapport de force équilibré ?

ANDY : Je serais tenté de dire que l'exposition sur la place publique de toutes ces données est une bonne chose parce que ça permet aux gens de comprendre qu'ils se servent de leur carte de crédit, ça laisse une trace. Certaines personnes trouvent ces débats très abstraits et ne comprennent pas bien où est le problème. Quand on leur mettra leurs propres traces sous les yeux, ils comprendront immédiatement.

JULIAN : Il suffit de demander, par exemple, la communication de l'intégralité de votre compte Facebook, qui contient environ 800 MB d'informations à votre sujet.

ANDY : On raconte qu'après la chute du Mur, quand le chancelier Kohl voulait réunifier l'Allemagne, les Américains ont posé une condition au cours de ce qu'on a appelé les conversations 2 + 4. Ils ont exigé de laisser le système de communication allemand sous leur contrôle, et Kohl pensait que ce n'était pas bien important parce qu'il ne comprenait pas vraiment de quoi il en retournait. Un de ses collaborateurs m'a raconté un jour que ça les inquiétait beaucoup, alors ils ont apporté dans son bureau deux caddies chargés de quelque 8 000 pages de retranscriptions d'appels téléphoniques interceptés par la Stasi et il a dit : « C'est quoi tout ça ? », et on lui a répondu : « C'est la totalité de vos communications téléphoniques des dix dernières années, y compris avec vos petites amies et votre femme, et votre assistante, et ainsi de suite. » Ça lui a fait comprendre ce qu'est l'interception des communications. Et c'est ça l'utilité des archives des services de sécurité : elles aident les gens à comprendre ce que fabriquent les services de sécurité. Donc, il y a des raisons d'être en faveur de leur ouverture totale, et si on votait tout de suite sur la question, je ne suis pas certain que je serais contre.

JULIAN : Ce n'est pas la question qui m'intéresse vraiment. Dans certains cas, par exemple si vous enquêtez sur la mafia, il est évidemment justifié de garder le secret pendant la durée de l'enquête. Dans certaines circonstances, on peut considérer que c'est légitime. Je ne dis pas pour autant que ce soit légitime en règle générale, je dis que c'est politiquement inévitable. Parfois, c'est une exigence politique pertinente, par exemple si on vous dit : « Ces types ont déjà tué, et ils préparent d'autres meurtres », alors quelle que soit votre position de principe sur la publicité des interceptions, elles resteront secrètes. C'est un combat perdu d'avance. Mais ce type de surveillance tactique a l'avantage d'être régulé en partie, on peut le limiter à un minimum d'individus. Quand on se sert d'interceptions tactiques pour des enquêtes judiciaires (et non pour du renseignement), c'est une manière d'obtenir des preuves. Les preuves finissent devant le juge, et donc devant le public. Il existe ainsi un certain contrôle sur ce qui se passe, au moins pendant une période donnée. Et le tribunal peut faire comparaître des gens à la barre pour évaluer si la manière dont les informations ont été obtenues était légitime. On garde un œil sur le processus. Mais la régulation des interceptions stratégiques est un non-sens. Puisque, par définition, il s'agit dès le départ de surveiller tout le monde, quelle législation pourra- t-on appliquer ?

JÉRÉMIE : Ce débat sur la publicité totale des informations me fait penser au groupe LulzSec, qui a rendu publiques toutes les données de 70 millions d'utilisateurs de Sony – on pouvait lire les adresses, les adresses mails, les mots de passe, etc. Je crois bien qu'il y avait même les informations de cartes de crédit. Moi qui milite activement pour la défense des droits fondamentaux, je me souviens d'avoir pensé : « Il y a quelque chose qui cloche. Si pour démontrer un fait ou simplement pour vous amuser, vous dévoilez les données personnelles des gens, ça ne va pas. » Cette histoire m'a mis très mal à l'aise. Je me suis dit : « Ces types ont voulu se moquer des services de sécurité informatique de Sony, ils ont voulu montrer qu'une compagnie réputée et puissante était incapable de garantir la confidentialité des données de ses utilisateurs, et qu'en voyant leur propre adresse mail ou leur nom dans ce listing les gens se diraient : "Merde, qu'est-ce qui m'a pris de confier toutes ces données à Sony ? C'est ça, ce qui se passe quand on confie ses données personnelles à une entreprise ?" »

JACOB : Et après, on tue le messager !

1. « Stasi still in charge of Stasi files », WikiLeaks, 4 octobre 2007 : http://www.wikileaks.org/wiki/Stasi_still_in_charge_of_Stasi_files (lien vérifié le 22 octobre 2012).

Des rats à l'opéra

JULIAN : Après avoir passé en revue tous ces scénarios pessimistes, j'aimerais qu'on envisage un scénario utopique. D'un côté, il y a la radicalisation de la jeunesse Internet, qui représentera bientôt

la plus grande partie de la jeunesse. De l'autre, on assiste à des initiatives désespérées en faveur de l'anonymat et de la liberté de publication, une opposition à toute forme de censure – et il existe toute une variété d'interactions de l'État avec le secteur privé pour s'y opposer –, mais supposons qu'on aboutisse au résultat le plus optimiste possible. À quoi cela ressemblera-t-il ?

JACOB : Je pense que le droit de lire et de s'exprimer librement s'applique à toute personne, sans exception. Cela vaut sans la moindre exception pour tous les êtres humains, et je fais exprès de citer Bill Hicks de travers1. Il parlait d'autre chose, de l'éducation, de l'habillement et de la nourriture, mais au fond c'est bien de ça qu'il s'agit : tout le monde a le droit de s'exprimer librement. Cela implique le droit de s'exprimer anonymement, le droit d'utiliser son argent sans interférence de tierces parties, le droit de se déplacer librement, le droit de corriger les données vous concernant qui se trouvent dans les systèmes. Il faut que tous les systèmes soumis à quelque autorité que ce soit fassent preuve de transparence et de responsabilité.

ANDY : J'ajouterais qu'avec l'explosion des systèmes de traitement de l'information et leur mise en réseau, avec la disponibilité d'outils comme Tor, avec la cryptographie et ainsi de suite, la quantité d'informations que l'on peut supprimer est assez limitée, ce qui veut dire que les gouvernements n'ont d'autre choix que de s'en charger, et ils en sont conscients. Ils savent qu'aujourd'hui le secret n'est pas une option viable à long terme, que tôt ou tard tout se retrouve sur la place publique, et c'est une bonne chose. Ça change leur façon d'agir. Ils savent qu'on pourra leur demander des comptes. Cela veut aussi dire qu'ils doivent faciliter l'apparition de lanceurs d'alerte internes, ce qu'a fait la loi Sarbanes-Oxley pour les entreprises cotées en Bourse aux États-Unis, en les obligeant à mettre en place une infrastructure d'alerte afin que les gens puissent dénoncer les agissements criminels ou les manquements à l'éthique de leurs supérieurs sans être sanctionnés par ceux qu'ils dénoncent2. C'est une bonne chose, et cela favorise la mise en place de processus durables, sur le long terme.

JÉRÉMIE : Pour aller dans le sens de Jacob, je pense que nous devons faire comprendre aux gens qu'un Internet libre, ouvert et universel est l'outil le plus important dont nous disposons pour faire face aux problèmes globaux qui se posent, et que sa préservation est l'une des tâches essentielles de notre génération. Quand quelqu'un quelque part – qu'il s'agisse d'un gouvernement ou d'une entreprise – restreint l'accès des gens à l'Internet universel, c'est Internet dans son ensemble qui est affecté. Ce sont les capacités de l'humanité qu'on limite. Or, il est possible d'agir ensemble pour rendre difficilement supportable le coût politique de ces décisions : tous les citoyens qui se retrouvent sur Internet peuvent aider à bloquer de telles tentatives. En tant que citoyens du Net, nous avons le pouvoir d'influer sur les décisions politiques et nous pouvons obliger nos élus et nos gouvernements à rendre des comptes quand ils prennent des décisions néfastes qui limitent nos libertés fondamentales et la liberté, la globalité et l'universalité d'Internet.

Tout cela demande à être développé. Nous devons continuer à diffuser notre savoir-faire. Nous devons continuer à améliorer nos moyens d'action, à partager nos tactiques de combat parlementaire pour garder les hommes politiques à l'œil et dénoncer l'influence des lobbies industriels. Nous devons continuer à développer des outils qui permettent aux citoyens de mettre sur pied leurs propres structures cryptées décentralisées, de posséder leur propre infrastructure de communication. Nous devons diffuser ces idées dans la société en tant que moyen de construire un monde meilleur, ce que nous avons déjà commencé à faire. Il s'agit simplement de poursuivre ce

travail.

JULIAN : Jacob, si tu penses par exemple à la manière dont quelqu'un comme Evgeny Morozov décrit les problèmes auxquels est confronté Internet, il est clair que les cypherpunks avaient déjà compris ces questions3. L'idée était qu'on ne pouvait pas se contenter de se plaindre de cette surveillance d'État en plein essor et ainsi de suite, mais que l'on pouvait, que l'on devait, en fait, construire les outils d'une nouvelle démocratie. Nous pouvons construire ces outils avec notre esprit, les diffuser et mettre en place une défense collective. La technologie et la science ne sont pas neutres. Il existe des formes particulières de technologie qui peuvent nous aider à obtenir des libertés et des droits fondamentaux auxquels les gens aspirent depuis très longtemps.

JACOB : Absolument. La chose la plus importante qu'il faut expliquer – surtout si l'on pense à un jeune de seize ou dix-huit ans qui rêve de bâtir un monde meilleur –, c'est que personne, ni ici ni ailleurs, ne sait en naissant quelles réalisations on inscrira sur sa pierre tombale. Nous sommes maîtres de nos choix. Tout le monde ici est maître de ses choix et tout le monde, surtout avec Internet, peut l'être dans le contexte de sa vie. Personne ne vous y oblige mais, si vous le souhaitez, vous pouvez le faire. Si vous le décidez, vous pourrez atteindre un nombre considérable de gens, surtout quand cela concerne Internet. Pour mettre en place des solutions, il faut d'abord faire des choix puis les partager, les populariser.

JULIAN : Donc, pour toi, si tu inventes quelque chose, tu peux le donner à un milliard de personnes pour qu'ils s'en servent.

JACOB : Ou si tu participes à la mise sur pied d'un réseau anonyme – le réseau Tor, par exemple –, tu contribues à mettre en place la possibilité de communications anonymes là où elles étaient inexistantes.

JÉRÉMIE : Il s'agit de partager cette connaissance librement et d'ouvrir des voies de communication que le savoir pourra emprunter librement, voilà de quoi il s'agit. Tor est un logiciel libre, et il se diffuse massivement aujourd'hui parce que nous incorporons cette notion de liberté dans la manière dont nous construisons nos possibles, notre technologie et nos modèles.

JACOB : Nous avons besoin de logiciels libres pour un monde libre, nous avons besoin de hardware libre et ouvert.

JULIAN : Quand tu dis « libre », tu veux dire sans restrictions, comme ça les gens peuvent bidouiller à l'intérieur, voir comment cela marche ?

JACOB : Exactement. Nous avons besoin de logiciels aussi libres que les lois d'une démocratie, où chacun a le droit d'étudier la loi, de la changer, de comprendre véritablement son but et de s'assurer qu'elle produit le résultat escompté. Logiciels libres, hardware libre et ouvert4.

JULIAN : Les cypherpunks avaient déjà formulé cette idée : « Le code, c'est la loi. »

JÉRÉMIE : C'est Larry Lessig qui a dit ça.

JULIAN : Sur Internet, ce que tu peux faire est défini par les programmes, les programmes qui tournent sur les machines, et donc, le code, c'est la loi.

JACOB : Exactement, et ça veut dire que tu peux construire des solutions, surtout en termes de programmation, mais aussi en termes d'impression 3D ou des choses sociales comme les espaces de hackers5. Tu peux aider à construire des solutions, ce qui est important c'est de les faire aboutir par un processus de normalisation : lorsque les gens auront pris l'habitude de construire leurs propres objets tridimensionnels, de modifier leurs propres logiciels, ils comprendront que si quelqu'un veut les en empêcher, quel qu'il soit, ce dernier ne devra pas être vu comme un fournisseur d'accès à Internet, mais comme un fournisseur d'accès à « Filtrenet » ou à « Censurenet »... qui ne respecte pas son obligation d'assurer la bonne marche du réseau.

Chacun d'entre nous ici consacre sa vie à ces questions, et il faut faire savoir aux gens qu'ils peuvent agir pour les générations futures autant que pour la génération actuelle. Voilà pourquoi je suis ici : si je n'apporte pas mon soutien à Julian, avec tout ce qu'on lui fait subir, quel monde suis-je en train de bâtir ? Quel message je fais passer lorsque je laisse une bande de porcs me bousculer ? Je ne me laisserai jamais faire, jamais. Nous devons bâtir, et nous devons changer les choses. Comme l'a dit Gandhi, « Soyez le changement que vous souhaitez voir dans le monde », mais soyez aussi l'empêcheur de tourner en rond que vous souhaitez voir dans le monde6. C'est une citation de A Softer World, ce n'est pas ce qu'a dit Gandhi, mais je pense que les gens doivent comprendre qu'ils ne peuvent pas rester assis à ne rien faire, il faut agir, et j'espère qu'ils comprendront7.

ANDY : Je pense qu'il y a de bonnes chances que les gens aillent bien plus loin, en fait, et que des solutions seront mises en avant par des gens insatisfaits de la situation et des options qui s'offrent à eux.

JULIAN : Si tu disais un mot à propos du Chaos Computer Club, dans ce contexte ?

ANDY : Encore et toujours le CCC... fnord8.

JULIAN : C'est parce que c'est unique au monde.

ANDY : Le CCC est une organisation galactique de hackers qui lutte pour la liberté d'information, la transparence de la technologie et qui s'intéresse à la relation entre développement humain et développement technologique, et donc à la relation entre société et développement.

JULIAN : Et tout ça est devenu politique, en fait.

ANDY : Le CCC est un peu devenu le forum des hackers, avec des milliers de membres basés, entre autres, en Allemagne – mais nous ne nous considérons pas comme des résidents allemands, nous nous considérons comme résidents sur Internet, c'est sans doute une des choses que les gens apprécient dans notre manière de voir. Nous avons des liens étroits avec des groupes de hackers en France, aux États-Unis et ailleurs.

JULIAN : Et pourquoi penses-tu que cela a démarré en Allemagne ? Le cœur est en Allemagne, et il s'est étendu au reste du monde.

ANDY : Les Allemands aiment que les choses soient bien structurées.

JÉRÉMIE : Rien ne vaut l'ingénierie allemande.

JULIAN : Mais il n'y a pas que ça, non ? C'est aussi lié à Berlin, à la chute du Mur.

ANDY : C'est le fruit de différents éléments. L'Allemagne a infligé des horreurs aux autres pays, alors il y a peut-être une plus grande résistance à l'idée que ça pourrait se reproduire, à faire la guerre par exemple. On a fait tout ça, on est passés par là, on a été durement punis et on a appris la leçon, et cette manière de penser décentralisée, ce comportement antifasciste, ce refus du totalitarisme, sont encore enseignés dans les écoles allemandes parce que nous en avons fait l'amère expérience. Donc, je pense que c'est en partie ce qui permet de comprendre le CCC, qui est un phénomène plutôt allemand. Wau Holland, un des cofondateurs du CCC, avait aussi une perception très politique de la question. Devant sa tombe, son père a dit des choses qui n'étaient pas agréables à entendre. Il a dit : « On ne verra plus jamais d'activités totalitaires, non pacifiques, sur le sol

allemand. » C'est ce qu'a dit le père en enterrant son fils, et pour moi cela explique en grande partie pourquoi Wau s'impliquait tellement dans le travail auprès des gens, pour les convaincre, les rendre meilleurs, diffuser les idées sans limitation, le tout dans un esprit de coopération, sans agressivité, pacifiquement.

L'approche participative – les mouvements open source et autres – a effectivement imprégné les cypherpunks américains, WikiLeaks et ainsi de suite. Aujourd'hui, c'est devenu global, avec des attitudes culturelles très différentes, très décentralisées, chez les hackers suisses, allemands, italiens, et c'est une bonne chose. Les hackers italiens n'agissent pas du tout comme des hackers allemands – où qu'ils se trouvent, ils adorent bien manger, alors que les hackers allemands ont surtout besoin que tout soit bien organisé. Je ne veux pas dire que l'un est meilleur que l'autre, je dis juste que chacune de ces cultures décentralisées a ses propres belles caractéristiques. Dans une conférence de hackers italiens, la cuisine est un endroit où l'on a envie de traîner, et dans une réunion de hackers allemands l'accès au réseau sera formidable, mais mieux vaut ne pas mettre les pieds dans la cuisine. Au centre de tout ça, il y a une créativité commune. Nous communions dans une sorte de conscience collective totalement indépendante de notre identité nationale, que l'on soit allemand, italien, américain ou n'importe quoi d'autre. Ce que nous voulons avant tout, c'est résoudre des problèmes, travailler ensemble. Pour nous, la censure sur Internet, le combat que mènent les gouvernements contre les nouvelles technologies, est comme un moment de l'évolution que nous devons surmonter.

Nous avançons dans la recherche des solutions, nous ne nous contentons heureusement pas de dénoncer des problèmes. Nous faisons face à toutes sortes d'obstacles, et cela risque de durer encore longtemps, mais nous voyons enfin émerger une génération d'hommes politiques pour qui Internet n'est pas une menace, un problème, mais une partie de la solution. Les armes font encore la loi sur terre, et le monde repose encore sur le pouvoir du secret et sur un certain modèle économique, mais tout cela change, et je pense que nous avons un rôle très important à jouer dans la définition des politiques. Nous sommes capables de débattre des problèmes par la controverse – c'est ainsi que le CCC procède depuis fort longtemps, en fait. Nous ne sommes pas un groupe homogène, de nombreuses opinions existent en notre sein. J'aime l'idée que nous discutions comme nous le faisons, sans avoir tout de suite réponse à tout. On s'interroge, on met nos idées sur la table et on voit ce qui se passe. C'est ça, le processus dont nous avons besoin, voilà pourquoi nous avons besoin d'un Internet libre.

JULIAN : Je vous ai demandé tout à l'heure quelle était votre vision optimiste du futur. La connaissance, la diversité, l'autodéterminaton grâce aux réseaux. Une population mondiale hautement instruite – je ne veux pas dire en termes d'études mais ayant une compréhension poussée de la manière dont fonctionne la société aux niveaux politique, industriel, scientifique et psychologique – résultant de la libre circulation des informations, stimulant l'épanouissement de nouvelles cultures et une diversification maximale de la pensée individuelle, une plus grande autodétermination régionale, et l'autodétermination de groupes d'intérêt capables d'agir rapidement en réseau et d'échanger de la valeur rapidement, par-dessus les frontières géographiques. C'est peut-être ce qui s'est passé au cours du Printemps arabe et pour l'activisme panarabe, lequel a été amplifié par Internet. Notre travail avec nawaat.org, qui, avec la création de TuniLeaks, a permis de contourner la censure et de diffuser les télégrammes du Département d'État dans la Tunisie prérévolutionnaire, a été une preuve éclatante de la puissance des réseaux pour porter l'information là où elle est nécessaire, et c'est très gratifiant, après tous les efforts que nous avons déployés, d'avoir pu contribuer à ce qui se passait9. Pour moi, cette lutte pour l'autodétermination n'est pas différente de la nôtre.

Cette évolution positive suppose que la société atteigne un certain niveau d'autocompréhension, parce qu'on ne peut pas supprimer le passé. Ainsi, grâce à la libre circulation de l'information, grâce à la capacité des gens à communiquer entre eux confidentiellement pour lutter contre toute dérive totalitaire, grâce à la libre circulation du microcapital qui pourrait quitter sans contrôle des zones devenues politiquement inhospitalières, plus aucun État néototalitaire ne pourrait se développer.

Sur ces bases, une grande variété de systèmes politiques est possible. Pour moi, l'Utopie serait une dystopie s'il n'y en avait qu'une. Les idéaux utopiques impliquent à mon sens une diversité de modèles et de systèmes d'interaction. Si on considère la façon dont les nouveaux produits culturels trouvent leur public, la façon dont évoluent les langues, la façon dont les sous-cultures forment leurs propres mécanismes d'interaction grâce à Internet, alors oui, je pense qu'une évolution optimiste, positive, est possible.

Mais, selon toute probabilité, je pense que les tendances à l'homogénéisation, à l'universalité, à la transformation de la société en un gigantesque marché vont de toute façon imposer les critères classiques du marché pour chaque service et chaque produit : il y aura un leader du marché, un autre en deuxième position, tel autre occupera une niche, et il y aura des retardataires qui ne pèseront pas lourd. Et pour que les interactions soient rapides et efficaces, cela passera sans doute par une homogénéisation massive du langage, une homogénéisation massive de la culture, bref une standardisation massive. Donc le scénario pessimiste me semble également probable, d'autant que la surveillance transnationale et les guerres de drones sont déjà là.

Un jour, j'avais resquillé pour voir Faust à l'opéra de Sydney. C'est un endroit très beau la nuit, l'architecture intérieure est somptueuse, des spots lumineux éclairent l'eau et le ciel. À la fin du spectacle, je me suis dirigé vers la sortie : il y avait là trois femmes accoudées à la rambarde qui discutaient en regardant la baie plongée dans l'obscurité. La plus âgée parlait de ses problèmes au travail, et j'ai compris qu'elle travaillait pour la CIA, que c'était un agent secret. Elle avait adressé une plainte au comité de supervision du renseignement du Sénat américain, elle racontait tout ça à voix basse à sa nièce et à une amie. Je me suis dit : « C'est donc vrai, ce qu'on raconte : les agents secrets fréquentent l'opéra de Sydney ! » Je me suis retourné et j'ai vu l'intérieur de l'opéra à travers les baies vitrées monumentales de l'entrée : un rat s'était introduit dans ce cadre super-raffiné et dévorait la nourriture qui traînait sur les buffets, bondissant sur les nappes blanches, sur le comptoir où il y avait tous les billets. Il avait vraiment l'air de s'éclater ! Pour moi, cette image décrit bien le scénario le plus probable pour l'avenir : une structure totalitaire contraignante, homogène, postmoderne, transnationale, incroyablement complexe, absurde et dégradante, avec, au cœur de cette complexité, des espaces où seuls les plus malins des rats parviendront à se glisser.

C'est le seul côté positif dans cette vision d'un futur globalement négatif : un État de surveillance transnational, quadrillé par des drones, un néoféodalisme en réseau d'une élite transnationale – non pas une élite au sens classique du terme, mais une élite résultant de l'interaction complexe produite par l'émergence de différentes élites dans différents pays, fusionnant sur le dos de leurs populations respectives.

Dans ce monde, toutes les communications seront surveillées, enregistrées, conservées pour toujours, pistées pour toujours. Dans ce monde, les individus et leurs interactions seront soumis au contrôle permanent de ce nouvel establishment, de la naissance à la mort. En dix ans à peine, la situation a déjà radicalement changé, nous y sommes presque. Je pense que ce sera une atmosphère étouffante de flicage permanent. Si toutes les informations recueillies sur la planète étaient publiques, le rapport de force serait rétabli et nous pourrions prendre en main notre destin, en tant que civilisation mondiale. Mais, sans des changements radicaux, cela n'adviendra pas. La surveillance de masse s'applique de façon disproportionnée à chacun de nous et accroît le pouvoir

de ceux qui en ont le contrôle, même si je ne suis pas certain que ce nouveau monde leur plaira à eux non plus. Il y aura une nouvelle course aux armements, le recours aux drones effacera les frontières telles que nous les connaissons, basées sur des caractéristiques physiques, et il en résultera un état de guerre permanent, à mesure que des réseaux d'influence triomphants imposeront leur loi au monde. Et, dans le même temps, les gens seront littéralement ensevelis sous les calculs sans fin de la bureaucratie.

Comment une personne normale pourrait-elle être libre dans un tel système ? La réponse est simple : c'est tout bonnement impossible. Bien sûr, la liberté totale n'existe pas, dans aucun système, mais les libertés dont nous a dotés notre évolution biologique, les libertés auxquelles nous sommes culturellement adaptés, disparaîtront presque entièrement. Je pense que les seules personnes qui jouiront encore des libertés qui étaient les nôtres il y a, disons, vingt ans (parce que l'État de surveillance en a déjà éliminé une bonne partie, même si nous n'en sommes pas encore pleinement conscients) seront des personnes possédant une compréhension exceptionnelle du fonctionnement du système. Une élite rebelle high-tech, à l'image de ces rats intelligents qui se promènent dans l'opéra.

1. « Voici ce que vous pouvez faire pour changer le monde, tout de suite, pour le mieux. Prenez tout l'argent que nous dépensons chaque année pour la défense et utilisez-le pour nourrir, habiller et éduquer les pauvres du monde. Cela suffira amplement, et nous pourrons explorer l'espace, ensemble, à la fois l'espace intérieur et extérieur, éternellement en paix », Bill Hicks. On peut le voir dire cela ici : « Bill Hicks – Positive Drugs Story » : http://youtu.be/vX1CvW38cHA (lien vérifié le 24 octobre 2012).

2. La loi Sarbanes-Oxley est une loi américaine votée en 2002 à la suite des scandales Enron, Tyco International, Adelphia, Peregrine Systems et WorldCom. Elle visait à mettre fin aux pratiques corrompues qui avaient conduit à ces scandales. La section 1107 de la loi, connue sous le nom USC 1513(e), stipule qu'il est criminel de prendre des mesures de rétorsion contre les lanceurs d'alarme.

3. Evgeny Morozov, The Net Delusion: The Dark Side of Internet Freedom, Public Affairs, 2011.

4. Sur les logiciels libres, voir « The Free Software Definition », sur le site Web GNU : https://www.gnu.org/philosophy/free-sw.html. Un hardware libre, ou un matériel libre, est un hardware qui n'est pas bridé par des brevets propriétaires, qui est construit conformément aux standards ouverts, lesquels permettent la rétro-ingénierie et le bidouillage, avec des principes de conception, des instructions et des plans librement disponibles, de sorte que tout utilisateur qui en a la capacité peut construire une réplique. Sur le hardware libre, voir aussi « Exceptionally Hard and Soft Meeting: exploring the frontiers of open source and DIY », EHSM : http://ehsm.eu. Voir également « Open-source hardware » sur Wikipédia : https://fr.wikipedia.org/wiki/Matériel_libre (tous ces liens ont été vérifiés le 24 octobre 2012).

5. Sur l'impression 3D avec du matériel libre et ouvert, voir la vidéo d'introduction de l'imprimante 3D RepRap : http://vimeo.com/5202148 (lien vérifié le 24 octobre 2012).

6. Cette phrase est extraite de A Softer World, a photographic webcomic :

http://www.asofterworld.com/index.php?id=189 (lien vérifié le 24 octobre 2012).

7. Pour approfondir la réflexion sur les questions abordées au cours de la discussion, Jacob recommande les deux ressources bibliographiques suivantes : « The Anonymity Bibliography, Selected Papers in Anonymity », sous la direction de Roger Dingledine et Nick Mathewson : http://freehaven.net/anonbib, ainsi que « The Censorship Bibliography, Selected Papers in Censorship », sous la direction de Philipp Winter : http://www.cs.kau.se/philwint/censorbib (ces deux liens ont été vérifiés le 24 octobre 2012).

8. Note volontairement laissée en blanc.

9. Nawaat.org est un blog collectif indépendant tunisien créé en 2004 : http://nawaat.org/portail. Tunileaks a été créé par Nawaat en novembre 2010, et a publié les télégrammes de WikiLeaks concernant la Tunisie : https://tunileaks.appspot.com. Pour plus d'informations sur Tunileaks et les tentatives de censure dont il a été victime de la part du régime de Ben Ali, voir « Tunisia : Censorship Continues as WikiLeaks Cables Make the Rounds », Global Voices Advocacy, 7 décembre 2010 : http://advocacy.globalvoicesonline.org/2010/12/07/tunisia-censorship-continues-as-wikileaks-cables-make-the-rounds (ces liens ont été vérifiés le 24 octobre 2012).