

BEN SCOTT

Conseiller principal, Open Technology Institute à la New America Foundation ; directeur des programmes, European Digital Agenda, Stiftung Neue Verantwortung

Nicolas Barré, directeur de la rédaction, Les Echos

Thank you, Luc-François. I am turning to you, Ben, and with you we will go to Europe, but with an American perspective. You are based in Berlin and as we all know, Germany is a country where data protection and privacy is very high on the agenda, especially since the Snowden affair, so what can you tell us about all this?

Ben Scott, Conseiller principal, Open Technology Institute à la New America Foundation ; directeur des programmes, European Digital Agenda, Stiftung Neue Verantwortung

Je vais adopter une perspective légèrement différente au sujet des big data. Je vais défendre devant vous l'idée que la première application majeure pour big data n'appartenait pas à Google, et elle n'appartenait pas à Amazon, la première application majeure pour big data appartenait à la NSA. La première fracture majeure dans le domaine de la politique étrangère et des relations internationales causée par les big data a été provoquée par Edward Snowden. Les conséquences de cette fracture ne vont pas seulement affecter la diplomatie internationale, elles vont affecter le développement des marchés internationaux de la technologie.

Car les big data, c'est le pouvoir, les analyses prédictives, et les analyses prédictives sont utilisées dans les affaires tout autant que dans le renseignement d'origine électromagnétique. Quand on vit un incident majeur comme l'affaire Snowden, on observe une sorte d'épidémie. La méfiance et le scepticisme que le public ressent quant à l'affaire de la NSA commencent à se propager dans les marchés d'affaires. En Allemagne, où je vis, l'affaire NSA est très vite devenue l'affaire Google. Posez-vous la question de savoir si le Parlement européen aurait passé une résolution pour briser Google sans Edward Snowden. Je ne pense pas. La relation entre ces deux phénomènes est une chose que nous, en tant que professionnels de la politique étrangère, devrions étudier avec attention.

Et où en sommes-nous 18 mois après les révélations de Snowden? La dernière fois que j'ai vu Thierry, j'ai parlé de Snowden, une semaine après les révélations. J'ai prédit à l'époque que si l'Europe ne prenait pas une place de leader pour modifier les politiques régulant les big data, ces politiques ne changeraient pas. Dix-huit mois après les révélations de Snowden, ce que nous avons, c'est rien. Le changement de politique le plus probable de la part de Washington et de Londres, c'est rien. C'est incroyablement frustrant pour les défenseurs des droits de l'Homme et des libertés civiles qui ont déposé des plaintes dans les tribunaux de toutes les grandes capitales du monde. C'est incroyablement démoralisant pour les populations des sociétés démocratiques qui font confiance à leur gouvernement pour gérer le pouvoir de façon responsable, mais ce n'est pas surprenant. Il n'est pas surprenant que la Realpolitik soit un adversaire de taille pour l'idéalisme dans le nouveau monde des big data.

La question est, les conséquences sont-elles aussi gérables qu'elles le paraissent ? Je pense que la plupart des dirigeants à la Maison Blanche, à Downing Street, dans toute l'Europe et la majeure partie de l'Asie ont décidé que les conséquences politiques de l'affaire Snowden étaient gérables politiquement. A court terme, l'excitation retombe. La plupart des États se sont adaptés en silence, s'ils n'avaient pas déjà accepté auparavant la réalité des big data comme instrument miracle des programmes de renseignement d'origine électromagnétique.

Cependant, j'aimerais vous proposer l'idée que les conséquences à long terme sont graves et qu'elles ne sont pas dans l'intérêt des gouvernements démocratiques. Quel message envoyons-nous au public si nous ne faisons rien pour gérer l'évolution moderne du concept de vie privée et les politiques de sécurité à l'ère numérique ? Le message que

nous envoyons à notre propre public, et je parle en tant qu'Américain, est, méfiez-vous de la technologie et méfiez-vous du gouvernement et quand les deux sont combinés, c'est le moment d'avoir peur. Ce n'est pas un message qui est dans notre intérêt à long terme, et à ce stade, on ne sait pas trop comment faire pour l'inverser.

Quel message envoyons-nous à l'international? J'aimerais vous soumettre l'idée que c'est le pire message, et que ses conséquences seront encore plus graves. Ce message, c'est que les gouvernements occidentaux ne respectent pas leurs propres principes, c'est un exemple supplémentaire que nous ne faisons pas ce que nous prôtons. Comment pourrions-nous justifier nos interventions dans les affaires du monde au nom de certains principes et de valeurs si nous permettons que notre propre sens moral d'être relativisé ? Les conséquences à long terme de ces changements sont importantes, et pourtant l'impact public de l'affaire Snowden sur les marchés de la consommation semble être négligeable.

Ainsi que vous venez de l'entendre de la part de mes deux très chers collègues, il y a un marché en expansion pour les big data. Vous avez tous encore vos téléphones portables alors même que vous savez que ce sont des appareils de traçage bruyants et clignottant. Vous continuez à utiliser les réseaux numériques pour vos communications personnelles. Nombre d'entre vous, ou au moins vos enfants, documentent leur vie sur les réseaux sociaux. Vous achetez tous des choses sur Internet. Peu d'entre vous, je parie, prennent la peine d'utiliser le chiffrement de bout en bout. Pourquoi cela ? C'est un paradoxe vexant. Il suggère que nous ne sommes pas aussi choqués par l'affaire Snowden que nous le disons, mais je pense que c'est une fausse piste. Je pense que c'est une fausse piste car je suis d'avis que nous n'accordons pas une confiance suffisante aux consommateurs. Réfléchissez un moment aux raisons pour lesquelles les consommateurs ne changent pas leur comportement. J'en vois trois. La première : « Je ne sais pas. Je n'ai rien lu concernant la NSA et je ne comprends pas comment fonctionne Internet et je ne vois pas que les technologies que j'utilise laissent des traces enregistrables de tout ce que je fais. » La deuxième « Je sais, mais je m'en moque. » Ceux-là sont les gens qui ont décidé que la culture de l'exhibition sur Internet est une chose à glorifier. Ou ceux qui croient que parce qu'eux-mêmes n'ont rien à cacher pour le moment, ils sont prêts à échanger la liberté contre la sécurité. Raison numéro trois : « Je sais ce qu'ils font, ça m'inquiète, mais que puis-je faire ? »

Le Centre Pew de Recherche Internet a récemment réalisé un sondage auprès d'Américains en posant des questions qui nous donnent certaines indications sur la répartition des gens dans ces trois catégories. Les résultats montrent que 5 % des Américains n'ont pas entendu parler de l'affaire Snowden. Je ne sais pas dans quelle grotte ils vivent. On trouve aussi que 91 % des Américains croient qu'ils ont perdu le contrôle de toutes les données qu'ils publient sur Internet. Et 80 % pensent qu'il est inquiétant que le gouvernement surveille leurs communications. Par conséquent, je suggère d'interpréter cela comme une preuve que la grande majorité des gens entre dans la catégorie 3 : « Je sais ce qui se passe. Je n'aime pas ça, mais que puis-je y faire ? Je ne peux pas éliminer la technologie de ma vie, elle est maintenant beaucoup trop intégrée. Cependant, je n'accorde aucune confiance au gouvernement pour protéger ma vie privée, donc je vis un paradoxe, et j'y reste au quotidien car je ne vois pas de meilleures options. » J'appelle cela le cynisme normatif.

Réfléchissez au changement dans la perception publique d'Internet qui nous a amenés au cynisme normatif. Pensez à où nous nous trouvons il y a trois ans lors du Printemps arabe. Les journaux rivalisaient de gros titres sur les révolutions Twitter. Bien entendu, c'était exagéré et en grande partie inexact, mais néanmoins, il y avait une conviction profonde qu'Internet était une technologie de libération, une infrastructure de communication décentralisée qui abaissait les barrières d'entrée dans les marchés des idées et du commerce. Et maintenant pensez à où nous sommes rendus – le cynisme normatif. En trois ans, nous sommes passés d'une technologie libératoire à la perception d'Internet comme une technologie de contrôle social et de manipulation politique. C'est une vision digne de Hobbes. Trois ans entre les révolutions libératoires de Twitter et le cynisme normatif.

C'est un problème, pour trois raisons. Un, sur le long terme, cela signifie la perte de foi dans les principes des gouvernements démocratiques dans notre pays et à l'étranger. Si nous ne faisons rien pour restaurer la légitimité des actions du pouvoir en ligne, nous le regretterons. Deux, cela signifie une perte de foi en la technologie. Même si je ne dis pas que vous allez balancer votre téléphone à la poubelle à la fin de mon intervention, je pense que vous serez hésitant, ou plus hésitant à adopter la prochaine génération de technologies. Cela va ralentir le rythme de l'innovation, ce qui n'est pas du tout dans notre intérêt. Et peut-être encore plus important, cela va interférer avec ce que j'appelle la banalité de la révolution technologique. La puissance d'Internet comme un agent de puissance douce ne réside pas

dans la révolution Twitter, ni dans la création d'un Google européen. La puissance d'Internet dans le monde, c'est l'effet cumulé de l'accès quotidien aux réseaux et marchés d'informations et de communication pour des milliards de gens. Ralentir ce développement technologique est une chose que nous devons faire avec beaucoup de prudence.

Que peut-on faire? Rétablir la confiance. Nous devons convaincre les gens qu'Internet offre plus d'avantages que d'inconvénients. Pas seulement aujourd'hui mais demain et dans 15 ans et pour cela, nous devons établir la légitimité, au moins pour les gouvernements démocratiques et leur comportement en ligne. Le public ne veut pas éliminer entièrement le pouvoir d'Internet, ce ne serait ni sage ni désirable. Le public veut être assuré que le pouvoir est utilisé sur Internet de façon légitime. Qu'il y a des règles contrôlant ce qui peut être fait et ce qui ne peut pas être fait, et qu'il y a une certaine transparence dans l'application de ces règles. C'est une modernisation du concept de vie privée et des politiques de sécurité que je crois nécessaire de mener de la part des gouvernements occidentaux au travers d'un agenda fondé sur les intérêts communs et pas comme une mesure de représailles ou de protectionnisme économique.

Je pense qu'il faut commencer en ne posant pas les questions les plus difficiles, comme par exemple, pouvons-nous harmoniser les politiques de surveillance internationales en respectant les traités des droits de l'homme? Si nous commençons par cette question, nous n'irons nulle part avant longtemps, et c'est ce qui s'est passé depuis 18 mois. Pour résoudre ce problème de légitimité, nous devons commencer par les questions faciles. Nous devons commencer avec les idées d'intérêt commun qui unissent au minimum les gouvernements démocratiques. Voici trois idées. D'abord, la transparence. Les gens ne sont pas choqués que les forces de l'ordre et les services de renseignement fassent leur travail pour assurer leur sécurité et celle du pays, ils veulent juste en savoir un peu plus sur comment cela se passe. Nous pouvons augmenter la transparence sans mettre à mal l'efficacité de nos services et nous pouvons harmoniser nos politiques de transparence de façon à ce que les alliés traditionnels se fassent confiance, en tout cas plus qu'ils ne se le font à l'heure actuelle. Deuxièmement, l'espionnage industriel. Le gouvernement des États-Unis dit ne pas en faire. Il y a très peu d'éléments dans les documents de Snowden suggérant qu'il en fait. Si les États-Unis n'en font pas et que la plupart des gouvernements démocratiques disent ne pas en faire, pourquoi ne pas écrire un traité multilatéral rendant l'espionnage industriel illégal? Pourquoi ne pas mener une campagne internationale pour établir des règles, des moyens de surveillance et des sanctions pour ceux qui font de l'espionnage industriel sur Internet? Des intérêts communs qui nous mettent sur la voie de la légitimité.

Enfin, et c'est le plus important, pour se reconnecter aux développements du marché, le problème le plus important à résoudre à court terme est la question de l'accès extraterritorial aux données. Par cela j'entends quelque chose de très simple, est-ce que le gouvernement des États-Unis peut aller sur Google et obtenir vos données si vous n'êtes pas citoyen des États-Unis et ne vivez pas sur le territoire des États-Unis? La grande asymétrie du marché technologique est le gros avantage des systèmes de renseignements américains, car la loi américaine impose que n'importe quelle entreprise opérant aux États-Unis a l'obligation de fournir des données quel que soit le pays dans le monde où se trouve son siège et qui que soit son propriétaire. C'est ce qui est franchement le plus problématique pour les pays européens, c'est ce qui perturbe l'alliance transatlantique, c'est ce qui fait obstacle au soutien des défenseurs de la vie privée pour le PTCL. Nous devons résoudre ce problème politiquement. Vous ne pouvez pas résoudre ce problème dans le marché. Vous ne pouvez pas demander aux entreprises de se prononcer sur comment répondre à des lois contradictoires quand elles enfreignent la loi soit dans le pays où elles opèrent soit dans le pays où elles font des affaires. C'est un problème politique et c'est un problème politique qui peut être résolu.

Sur cette base, nous pouvons commencer à construire un agenda modernisé sur les questions de vie privée et de politique de sécurité de façon à ce que les big data soient à nouveau envisagées comme une technologie de progrès, une technologie libératoire, une idée passionnante, qu'elle soit entre les mains du secteur privé ou entre les mains du secteur public. Nous nous éloignons alors d'une conception d'Internet à la Hobbes, qui ne colle ni avec la politique étrangère des États-Unis, ni avec celle d'aucune nation démocratique. Merci beaucoup.