

Analyse des débats

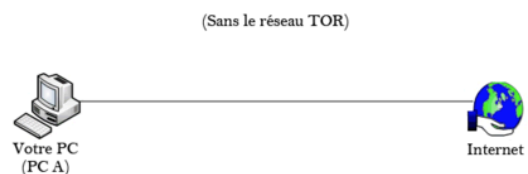
Tor : Outil de protection des données personnelles ou porte d'entrée vers les réseaux troubles ?

Qu'est-ce que Tor (The Onion Router) ?

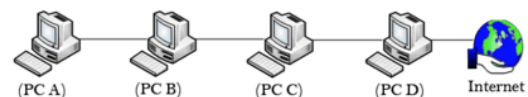
Tor est un réseau en ligne permettant de préserver l'anonymat des personnes sur Internet tout en naviguant sur le Web, en publiant des sites et en communiquant avec les autres. Le principe de fonctionnement qui donnera plus tard naissance à Tor a été développé au milieu des années 1990 par le mathématicien Paul Syverson et les informaticiens Michael G. Reed et David Goldschlag avec l'aide des employés de l'United States Naval Research Laboratory. Leur but premier était de protéger les communications des écoutes et analyses de trafic. Syverson, Roger Dingledine et Nick Mathewson développent la version alpha de Tor et lancent le projet en septembre 2002. Diverses améliorations de Tor se sont ensuite succédées.

Quel est son fonctionnement ?

Les communications sont acheminées de façon aléatoire, via un réseau de proxys¹ indépendants et bénévoles. Tout le trafic entre les serveurs Tor (ou relais) est crypté, et chacun des relais ne connaît que l'adresse IP de deux autres – celui qui le précède immédiatement et celui qui le suit immédiatement dans la chaîne. Le nom Tor vient de ce principe ; de même que les différentes couches d'un oignon n'ont un contact qu'avec les couches immédiatement inférieures et supérieures, un relais n'a d'information que sur le relai qui le précède et le relai qui le succède.

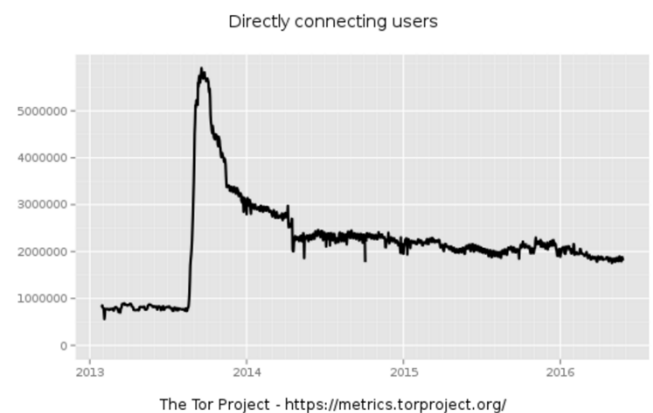


Connexion TOR



Les débuts de la controverse

La controverse autour de Tor n'apparaît dans les médias qu'assez récemment. Ce n'est que dans les 3 ou 4 dernières années que le débat autour de Tor s'est intensifié. En Juin 2013, suite aux révélations d'Edward Snowden, on a pu constater une augmentation de l'utilisation de Tor ; un réflexe naturel des internautes souhaitant se protéger de la surveillance des gouvernements. Tor est alors sous les projecteurs. Mais quelques mois après, en Octobre 2013, la fermeture du site Silk Road (site de vente de produits illicites : armes, drogues, etc.) fait de l'ombre à Tor. Une constatation dénoncée par les médias : Tor peut également couvrir des ventes illicites, des activités illégales. Le débat se poursuit dans les années



1. **Proxy** : composant logiciel informatique jouant le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges. (Source : *Wikipédia*)

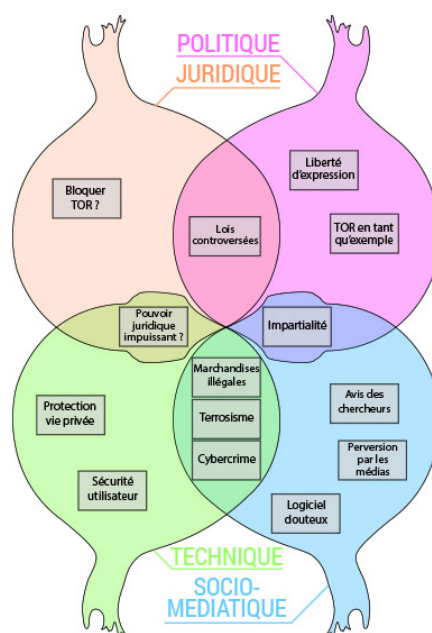
qui suivent ; les gouvernements conscients du danger que peut représenter Tor expriment leur inquiétude en faisant approuver des lois, pour avoir une plus grande emprise sur les données informatiques, sans toutefois interdire l'usage de Tor.

Un autre pan de la controverse concerne la montée de la logique sécuritaire (avec par exemple la loi renseignement de Juillet 2015). Cette montée a été accélérée en France par les récents attentats terroristes (attentats de Janvier 2015 et du 13 novembre 2015). Devant cette montée, l'objectif premier de Tor est remis en avant : protéger la vie privée et préserver le principe de navigation anonyme sur internet. C'est la volonté des fondateurs, des développeurs de Tor et des utilisateurs que l'on pourrait qualifier de lambda. Un extrait de l'interview de Lunar², un des rares développeurs français à travailler à plein temps sur Tor, illustre cette idée : « La fin de l'anonymat du lecteur pose un gros problème de société. Tous ces acteurs différents peuvent savoir et enregistrer le fait que j'ai consulté certaines informations. Dans une bibliothèque, je peux emprunter n'importe quel livre, le lire ou le ramener chez moi sans mettre grand monde au courant. Si je sais qu'il y a un risque que je sois surveillé dans mes lectures, je ne vais pas me permettre d'aller vers les mêmes informations. Cela revient à une forme de négation de la liberté de pensée. C'est une censure sur l'objet même de notre curiosité. »

Un outil aussi puissant que Tor soulève nécessairement des questions, des débats. Est-ce que Tor est un outil qui permet la protection de la vie privée, autrement dit un outil qui permet de naviguer sans trace, ou est-ce plutôt une porte vers les réseaux troubles, vers l'Internet incontrôlé ?

A partir de cette problématique, quatre principaux blocs vont se former et faire émerger des questions. Chacun de ces blocs représente un aspect de la controverse de Tor. Toutefois, il faut garder à l'esprit qu'aucun de ces blocs n'est indépendant des autres, ils communiquent à travers différents débats. Nous le verrons par la suite.

La sphère juridique représentera tous les débats qui font intervenir la législation, la sphère politique présentera l'intérêt ou les problèmes que peut susciter Tor dans une nation, la sphère socio-médiatique présentera la vision de Tor selon les médias et enfin la sphère technique éclaircira les possibilités et les frontières de Tor.



2. VACARME. TOR, la face chiffrée d'Internet entretien avec Lunar. [En ligne] Disponible sur : <http://www.vacarme.org/article2681.html>

Présentation des principaux débats :

a) Est-ce que le pouvoir Juridique est impuissant ?

Cette éventuelle impuissance se retrouve dans deux aspects importants : l'aspect juridique et l'aspect technique.

D'un point de vue juridique, est-ce que la loi peut faire quelque chose face à Tor, est-ce qu'elle peut le bloquer ? Il semblerait a priori que dans certains cas ce soit possible, par exemple en France, en cas de terrorisme : d'après la loi n° 2015-1501 du 20 novembre 2015 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et renforçant l'efficacité de ses dispositions : « Article 11.II. - Le ministre de l'intérieur peut prendre toute mesure pour assurer l'interruption de tout service de communication au public en ligne provoquant à la commission d'actes de terrorisme ou en faisant l'apologie. ». Mais un extrait d'une interview d'une de mes camarades avec Félix Tréguer, membre fondateur de La Quadrature du Net, peut nous éclairer sur ce point :

« Nesrine Kortas : Interdire TOR en France aujourd'hui serait-il une chose possible à votre avis ? La loi relative à l'État d'urgence pourrait-elle un jour justifier le blocage du réseau par exemple ?

Félix Tréguer : Cette loi permet le blocage des sites promulguant le terrorisme (comme djihadiste.com) et non les communications TOR. En fait, le serveur d'une personne utilisant le réseau a été utilisé pour faire une fausse annonce à la bombe auparavant. Elle a refusé de coopérer avec la police pour qu'ils accèdent à son disque dur. La police n'a pas pu prouver quoi que ce soit. Aujourd'hui, on ne va pas arrêter des personnes dont les serveurs ont servi d'intermédiaires pour transmettre une information. » On constate alors que les lois ont leurs limites ; il y a toujours cette tension du côté de l'état entre garantir la sécurité et respecter les libertés.

Et d'un point de vue technique est-il possible d'arrêter Tor ? Tor repose sur la coopération entre tous ses utilisateurs ; plus il y aura d'utilisateurs et plus il sera difficile de bloquer son utilisation. Un extrait de l'interview d'un de mes camarades avec Marie³ (auparavant cryptologue), travaillant à la CNIL (Commission nationale de l'informatique et des libertés) dans la protection de la vie privée, explique pourquoi il est difficile d'arrêter Tor :

« Vincent Jarasse : Est-ce que l'on peut techniquement bloquer TOR ? Selon la presse, la Chine l'aurait fait.

Marie : La question c'est combien de temps. Il y a un principe de base de TOR, mais il y a énormément d'innovations en continu. Donc même si la Chine arrive à bloquer TOR à un instant t, à l'instant t+dt des évolutions auront été apportées pour contourner ce blocage. Mais en réalité la Chine ne ferme pas TOR. Ce qu'elle fait c'est faire en sorte que ça ne passe pas le firewall chinois. En soi, on pourrait très bien faire fonctionner TOR au sein de la Chine, mais l'intérêt est limité. Concernant le blocage, comme je l'ai dit, les développeurs du projet TOR s'adaptent. A quoi reconnaît-on que du flux sortant d'un serveur est du flux TOR ? En fait il y a une empreinte propre au code TOR. Lorsque cette empreinte est identifiée comme du code TOR, il « suffit » de modifier cette empreinte pour être de nouveau indétectable... »

On observe ici cette double difficulté pour contrôler Tor.

3. Dans un souci d'anonymat, on ne révélera pas son vrai nom.

Les acteurs impliqués ici sont les instances juridiques qui mettent de nouvelles lois en place et les utilisateurs de Tor qui pourraient aller à l'encontre de ces lois. L'un mettant en exergue le danger que Tor représente et l'autre les avantages de Tor. Ceci nous amène à un autre débat : est-il courant que Tor soit utilisé pour enfreindre la loi ?

b) Est-ce que l'utilisation de Tor pour commettre des actes illégaux, des crimes est courante ?

Les médias présentent parfois Tor comme un logiciel mystérieux permettant la vente de marchandises illégales, le terrorisme et facilitant le cybercrime. Si bien que Tor a une mauvaise image auprès d'une partie du grand public et qu'il apparaît comme un logiciel douteux permettant l'anonymat sur Internet et qu'il est souvent utilisé à de mauvaises fins. Mais qu'en est-il en réalité, est-ce vraiment l'usage principal de Tor ?

Des chercheurs (Département des études militaires de King's College) se sont penchés sur le sujet et leur conclusion est qu'il n'y a qu'une partie infime des adresses en .onion dont le contenu est en rapport avec des activités terroristes⁴.

Des recherches qui ne concernent pas directement Tor mais qui permettent d'avoir une idée existent : Loi n° 2015-912 du 24 Juillet 2015 relative au renseignement a pour but de renforcer le cadre juridique national du renseignement en France. Elle prévoit de mettre en place certaines mesures. Ces mesures peuvent porter atteinte à la vie privée. Par exemple, ces mesures comprennent l'installation chez les opérateurs de télécommunications de dispositifs, les « boîtes noires », qui permettraient de détecter des comportements suspects à partir de données de connexions. D'après Daniel Le Métayer et Claude Castelluccia, directeurs de recherche à l'Institut national de recherche en informatique et en automatique (Inria), spécialistes en protection de la vie privée, la probabilité d'atteindre un terroriste avec ces dispositifs ne serait que de 0.5% : on espionnerait ainsi 99.5% personnes autres personnes sans raison.⁵

Les acteurs impliqués ici sont les médias qui ne donnent parfois au grand public qu'une image partielle de Tor et les chercheurs qui montrent que l'usage à craindre n'est que minoritaire.

Et enfin, le dernier acteur est incarné par les instances juridiques qui pose la question citée en titre.

c) Quelle est la place de Tor dans la politique ?

Pour certains, TOR représente un outil qui permet la liberté d'expression, l'interdire dans un pays serait donc un message très fort et controversé. L'exemple souvent cité est celui de la Chine dont le gouvernement a bloqué Tor. Les autres pays ne veulent pas se calquer sur la Chine et essaient donc de ne pas interdire l'utilisation de Tor. Au-delà des moyens techniques permis par Tor, celui-ci est devenu un symbole de liberté d'expression ; il permet de contourner la censure, d'échapper à la dictature et de parler librement. Deux exemples :

- Révolutions au printemps arabe, soulèvement en Syrie où les rebelles ont organisé la lutte sur Tor sans avoir à s'inquiéter.
- ONG : « Reporters sans frontières » : défend la liberté des journalistes sur toute la planète et recommande à ses journalistes l'utilisation de Tor pour travailler librement en sécurité.

4. Voir l'article en ligne : <http://www.numerama.com/politique/157605-une-etude-trouve-peu-de-traces-de-terroristes-sur-le-dark-net.html>

5. Voir l'article en ligne : *Le Monde* (Interview) : http://www.lemonde.fr/pixels/article/2015/05/06/loi-renseignement-des-dizaines-de-milliers-de-personnes-vont-etre-suspectees-a-tort_4628392_4408996.html

Tor ? En septembre 2014, internet dépasse un milliard de sites pour près de trois milliards d'internautes. Avec l'expansion de l'Internet vient l'expansion de Tor qui rappelons-le, grandit avec chaque utilisateur qui le rejoint. Tor grandit de plus en plus, il devient de plus en plus difficile à arrêter.

Novembre 2014, une opération affecte Tor, l'opération Onymous : c'est une action internationale coordonnée des forces de police visant à ébranler un marché illégal gangrénant Tor⁸. Une coalition d'unités de police dans 16 pays (dont la France) avec le FBI, Europol et d'autres agences ont procédé à l'arrestation de 17 individus soupçonnés d'organiser des trafics d'armes et de drogues sur le Darknet. 410 services ont été suspendus. Cette affaire ternit l'image de Tor qui apparaît comme un outil utilisé par des criminels.

Et en 2015, la loi relative au renseignement est promulguée ; cette loi montre indirectement la position du gouvernement vis-à-vis de Tor.

Décembre 2015, la police exprime son souhait d'interdire les connexions au réseau Tor. En Février 2016, une personne utilisant un relais Tor est arrêtée parce que son serveur a été utilisé pour faire des fausses menaces à la bombe. Cette fois c'est la police, et donc le pouvoir exécutif, qui exprime sa position vis-à-vis de Tor.

Liens entre les différents acteurs

Il n'y a pas une réelle alliance entre les gouvernements et les médias mais ils sont obligatoirement corrélés ; les gouvernements expriment leur réticence devant Tor et les médias vont souvent dans leur sens en rappelant des événements marquants (Ex : Silk Road, Opération Onymous, etc.). Le gouvernement chinois a lui par contre décidé de bloquer Tor.

Le pouvoir exécutif et le pouvoir législatif s'allient à travers la police et le gouvernement ; la volonté des deux parties étant de lutter contre les crimes qui peuvent naître de Tor (Exemple du lycéen de Dijon qui a utilisé Tor ; application de l'article 434-15-2 du code pénal punit de 3 ans de prison et 45 000 euros d'amende le fait, « pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités »).

Les créateurs de Tor défendent évidemment leur création et s'allient avec les utilisateurs pour défendre leur liberté d'expression et leur vie privée. Les chercheurs vont souvent dans le sens des utilisateurs également puisque toutes leurs recherches amènent à penser que Tor n'est pas utilisé pour des mauvaises fins. Parmi les utilisateurs, on comprend les utilisateurs « lambda » mais également les journalistes inquiétés par des gouvernements autoritaires.

Conclusion :

Tor suscite des débats autant au niveau national qu'international comme on a pu le constater dans l'Opération Onymous.

Les différents acteurs s'expriment sur divers terrains. Comme on a pu le voir, les développeurs et les membres d'association comme La Quadrature du Net font des interviews pour démontrer la vertu de leur travail (protection de la privée, liberté d'expression). Les internautes lambdas veulent protéger leur vie privée et expriment parfois leur mécontentement à l'égard de certaines lois, directement sur l'Internet ou également à l'aide des médias. Les gouvernements et la police expriment avec l'aide de certains médias, leurs craintes devant les

8. Voir l'article en ligne : http://www.lemonde.fr/pixels/article/2014/11/11/les-coulisses-de-l-operation-onymous-contre-des-dizaines-de-sites-caches-illegaux_4521827_4408996.html

activités illégales permises par Tor. Ils font également comprendre leur position de façon indirecte en faisant adopter de nouvelles lois. On a pu voir les liens qui existent entre Tor et certaines lois comme la loi renseignement. Tor n'a peut-être pas été évoqué directement à l'assemblée nationale mais l'argument de protection de la vie privée a été évoqué pour s'opposer à la loi renseignement⁹ : un exemple avec Laure de la Raudière : « ... L'article 2, dans le cadre de la lutte contre le terrorisme, met en place des techniques qui collecteront massivement des données bien au-delà des personnes ayant l'idée de devenir djihadistes. ». Les acteurs de la controverse de Tor sont donc divers, et s'expriment sur des terrains différents et certains d'entre eux participent à la controverse de façon indirecte (par exemple les acteurs politiques qui expriment leur opinion sur la loi renseignement).

9. Voir l'article en ligne : <http://www.numerama.com/magazine/32809-l-assemblee-adopte-les-boites-noires-qui-surveilleront-votre-comportement.html>