Interview avec Félix Tréguer, membre fondateur de l'association La Quadrature du Net qui est une association de défense des droits et libertés des citoyens sur Internet fondée en 2008.

1/ Que pensez-vous du cadre juridique qui régule les pratiques de surveillance par l'Etat sur Internet?

Depuis le début des années 2000, l'État et les organismes des pays occidentaux ont développé des capacités pour améliorer les pratiques de surveillance. Des milliers de dollars ont été consacré pour cette finalité.
Il y'a eu quelques évolutions du droit à ce sujet. Par exemple en France, il y'a une loi qui date de 1991 relative au secret des correspondances émises par la voie des communications électroniques.
(Le secret des correspondances émises par la voie des communications électroniques est garanti par la loi.
Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci.)

Cette loi imparfaite a été modifiée au fur des années. Et depuis se sont développées de nombreuses pratiques relatives à l'accès aux métadonnées notamment l'installation de mouchards (boites noires) chez les opérateurs téléphoniques.
Depuis le début des révélations Snowden en Juin 2013, la nécessité d'améliorer le cadre juridique concernant ces pratiques devient évidente. Pour se protéger des éventuels procès et scandales, les États ont cherché à améliorer les lois qui leur permettent de continuer leurs pratiques. C'est l'exemple de loi relative au renseignement en France.

2/ Dans vos articles, vous dites que les attentats terroristes à Paris ont été utilisé comme un prétexte pour légaliser les pratiques de surveillance.

En effet, la surveillance est un sujet sensible pour les gouvernements. Une anecdote intéressante est qu'en 1974, un ingénieur en informatique au ministère de l'intérieur en France est allé voir un journaliste du Monde et lui a parlé du système permettant de regrouper des fichiers de surveillance. Ce fut un grand scandale et ça a aboutit à une loi 4 ans plus tard : loi liberté et informatique. L'État Français sait très bien qu'il faut améliorer le cadre juridique permettant la surveillance pour éviter les scandales. Le projet de loi à ce sujet existe avant les séries d'attentats à Paris. Il a été retardé par les révélations Snowden.

En 2006 l'accès aux métadonnées a été légalisé dans le but de la lutte contre le terrorisme et cela a été facile à légitimer. Juste après les attentats à Madrid et Londres (2004-2005) le contexte du terrorisme était en avant de la scène mais on sait maintenant qu'ils ont continué à accéder aux données même après.

Aujourd'hui, la loi sur le renseignement en France semble légitime mais en fait elle permet de scanner des communications de personnes qui n'ont rien à voir avec le terrorisme. Des experts ont même démontré que le programme utilisé a un taux de fausse positivité alarmant ce qui va mettre les services de renseignement sur des fausses pistes.

3/ Pour justifier le recours à la loi de renseignement justement certains disent que ceux qui n'ont rien à cacher ne doivent pas se soucier de cela. Que pouvez-vous dire à ces personnes?

Déjà c'est un faux argument. On a toujours quelque chose à cacher. On a des secrets et c'est légitime.
Dire que je m'en fou que ma vie privée soit compromise parce que j'ai rien à cacher c'est comme dire j'ai rien à faire de la liberté d'expression parce que j'ai rien a dire.
C'est important que les individus puissent se cacher et se protéger de l'État et de préserver cette capacité de cacher quelque chose.
Il est possible que demain Marine Le Pen arrive au pouvoir et si on veut lancer un mouvement de résistance on pourrait être bien embêtés.
Il ne faut jamais oublié qu'un État qui a des pouvoirs illimités sur ses citoyens est dangereux.

Il ne faut pas oublier aussi que chaque citoyen a le droit de se protéger des organismes qui cherchent à faire de la publicité. Par ailleurs, les directeurs des grandes entreprises doivent être capables de se protéger de la concurrence.

4/ Pensez-vous que le réseau TOR est un outil efficace pour se protéger de l'Etat et préserver sa vie privée ?

C'est difficile à dire parce qu'on ignore les capacités de surveillance de l'Etat. Il y'a des rumeurs qui disent que les flux d'informations et de communications sur le réseau TOR sont stockées par l'État même si ce dernier ne peut les lire pour le moment. Il faut se méfier du coup en utilisant TOR parce qu'il pourrait qu'un jour pas très loin l'Etat puisse déchiffrer les communications. Par suite, en utilisant le réseau, on peut être surveillé davantage.
Par ailleurs, Il est possible d'attaquer aujourd'hui le réseau TOR. Les services de renseignement peuvent surveiller un relais suspecté d'être un serveur du réseau. En observant les entrées et sorties, on peut savoir d'où la communication a été émise. Ce modèle d'attaque ne fonctionne que lorsqu'il y'a un nombre limité de serveurs relais.

Après les révélations Snowden, 30 % des citoyens en Allemagne ont déclaré avoir changé leurs pratiques. Que ce soit commencer à utiliser le chiffrement ou simplement changer les paramètres de sécurité de leurs comptes FB.
Les personnes qui travaillent pour l'association nos oignons dont le but est de promouvoir le réseau TOR pourront répondre à cette question de façon plus développée.
Personnellement je pense que les personnes qui travaillent sur TOR sont honnêtes et cherchent à améliorer la protection des vies privées.
TOR reste une technique parmi d'autres. Ce qui est important c'est d'apprendre aux citoyens comment bien protéger leurs données.

5/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 ?

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 ne peut pas les interdire d'arrêter leurs activités.

Ces personnes jouent simplement le rôle des opérateurs téléphoniques. Par exemple aujourd'hui, il y'a un gros débat depuis 2 mois aux États-Unis parce que la police cherche à accéder aux données sur l'iPhone d'un terroriste qui a tiré sur des personnes. En fait, il faut savoir que depuis les révélations Snowden Apple a amélioré la protection des données privées sur leurs appareils. Le FBI cherche à contraindre la société à faire collaborer certains de ses ingénieurs afin de déchiffrer le code sur le téléphone de l'homme. Apple a refusé. Et l'ancien président du NSA a pris la défense de la société ce qui est surprenant vu qu'il a financé des recherches pour contourner le chiffrement et les mécanismes de protection.