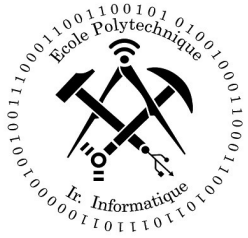
INFO-F510 – Information Technology in Society
Protection de la vie privée via l'anonymat

Gilles Degols, Brian Delhaisse, Quentin Delhaye et Anonymous



Année académique 2014 - 2015

Table des matières

1 Introduction

> *"It turns out that it's easier in this universe to encrypt information, much easier than it is to decrypt it if you're someone watching from the outside... the universe fundamentally favours privacy."*
>
> Julian Assange

Les progrès technologiques qui ont marqué l'Histoire humaine ont eu de nombreux impacts, soit positifs, soit négatifs, mais la plupart du temps ils étaient une combinaison des deux. Avec l'avènement de l'internet, le monde entier a pu bénéficier d'avantages en découlant : un nouveau secteur économique, accéder à des marchés étrangers facilement, partager ses connaissances, ... Le côté positif a montré sa face et est resté ancré dans le subconscient de la plupart des individus : « l'internet c'est l'avenir ». Oui, mais... à quel prix ?

Nous avons cru que l'anonymat était le propre de l'internet et que celui-ci nous permettrait encore longtemps de nous exprimer et nous renseigner sans que le gouvernement ou que quiconque puisse nous enlever ces droits. Les récents événements impliquant la NSA [24], mais aussi Facebook et autres réseaux sociaux nous ont montré que justement l'anonymat n'est plus un droit acquis : c'est un droit en sursis.

Quelques voix s'élèvent au sein de l'Union Européenne pour essayer de protéger le droit à l'anonymat et à la vie privée sur internet [8], mais celles-ci ne semblent être que des bouées perdues apparaissant au gré des scandales et disparaissant tout aussitôt.

La protection de la vie privée sur le web est-elle indispensable ou bien la source de problèmes divers ? Tout au long de ce dossier nous allons tenter de mesurer l'importance de cet anonymat, au niveau des individus mais aussi son impact sur un pays.

Pour cela, nous allons tout d'abord commencer par un historique de l'anonymat sur internet. Nous décrirons ensuite explicitement ce qu'est l'anonymat et les différents types existant sur l'internet. La section suivante décrira les avantages et désavantages de cet anonymat. Nous analyserons ensuite successivement les sujets les plus populaires où l'anonymat est utilisé, et nous discuterons de la possibilité d'être parfaitement anonyme sur l'internet ou s'il existe toujours un moyen de trouver l'identité d'un individu. Nous terminerons par parler brièvement des lois existant sur l'anonymat sur les différents continents, et conclurons avec l'utilité de l'anonymat sur l'internet.

2 De l'inconnu au profilé

Avec l'avènement du web et l'apparition des forums et blogs, il est devenu de plus en plus facile pour tout un chacun de partager son avis sur différents sujets, et ce, sans même avoir de connaissances poussées en informatique [1]. L'anonymat était assuré par de simples pseudonymes sans nécessité de donner un nom complet ou une adresse pour communiquer. À ce moment-là il ne se posait pas de problèmes majeurs en terme d'anonymat étant donné que chaque forum et blog avait une portée relativement limitée en terme d'audience. De ce fait, seules les autorités pouvaient montrer un intérêt particulier à essayer de lever l'anonymat sur des internautes lorsque des messages avaient un contenu contraire aux lois.

1. À ce sujet, Justin Kruger et David Dunning [15] ont publié un article très intéressant en 1999 sur la difficulté d'un individu de prendre conscience de sa propre incompétence dans un domaine donné. L'accès à une pléthore d'information sans l'éducation parfois nécessaire peut aujourd'hui exacerber cette incompétence, un quidam anonyme pouvant s'auto-proclamer expert dans n'importe quel domaine.

De nos jours, néanmoins, des géants du web ont fait leur apparition. Tout d'abord les moteurs de recherches qui avaient pour vocation d'améliorer leurs résultats de recherche (en plus de l'objectif publicitaire) commencèrent à grignoter petit à petit sur le sacro-saint anonymat. En effet, comment améliorer ses résultats de recherches si ce n'est en mesurant les habitudes d'un même utilisateur ? En sachant qu'il a l'habitude de cliquer sur des liens d'un certain site, il serait tout à fait logique de les lui présenter à l'avenir. Un enregistrement des données relatives à une adresse IP (Internet Protocol), ainsi que sur des cookies ajoutés par le moteur de recherche permettent ainsi facilement de créer petit à petit un profil basique de l'utilisateur, rendant celui-ci légèrement moins anonyme. Il n'est pas encore question de trouver qui se cache derrière ce profil, cela n'a pas d'intérêt immédiat pour la plupart des entreprises. Mais par la création de ce genre de profil, on est passé d'un utilisateur quelconque à un utilisateur profilé. Et comment accroître ses revenus publicitaires facilement si ce n'est en reconnaissant de façon unique l'internaute utilisant son site internet, et ainsi pouvoir le contacter avec des offres intéressantes ?

Arrivent alors les réseaux sociaux. Avec un profil unique pour une même personne, ceux-ci sont le paradis des annonceurs qui veulent cibler au mieux les internautes susceptibles d'acheter leurs produits. Facebook en est l'exemple parfait, bien que d'autres acteurs du web s'y essaient aussi (comme Google). Avec un compte Facebook par personne, et plus de 1 milliard d'utilisateurs actifs [9], cela montre que nombre de personnes sont prêtes à abandonner, ne serait-ce que temporairement, leur anonymat en échange d'un service particulier.

Le problème qui se soulève alors n'est plus seulement ce dont l'utilisateur a conscience et accepte sciemment, comme l'accès à un service quelconque, mais ce qu'on lui impose sans qu'il ne soit nécessairement au courant ou qu'il n'en tire un intérêt direct. Nous pouvons citer le cas des modules Facebook qui sont utilisés sur de nombreux sites, ceux-ci sont utilisés pour commenter des articles, s'inscrire à de nouveaux sites, et de nombreuses fonctionnalités ayant pour but d'identifier l'utilisateur. Nous n'avons dès lors plus le choix de garder notre anonymat sur les pages que nous visitons, les développeurs ayant décidé de sacrifier notre anonymat pour faire quelques économies lors de la création de leur site.

Nous sommes désormais passés à une phase où une règle d'or semble se dessiner petit à petit à travers l'internet : *Vous voulez un service performant ? Dites-moi qui vous êtes !*. Il existe souvent d'autres services similaires accessibles sans décliner son identité, mais ceux-ci ont tendance à être relégués au fin fond de la toile.

Cependant, la levée progressive de l'anonymat vient aussi d'une volonté de sécurité et de contrôle de la part des autorités. En effet, un anonymat intégral rime avec une impunité totale, ce qui n'est pas viable dans une société structurée autour de lois, de droits et de devoirs. Les arguments généralement avancés contre l'anonymat sont la diffamation [27], ou la sempiternelle identification de potentiels terroristes [5] qui resurgit à chaque attaque. Nous reviendrons plus loin sur les désavantages qu'entraînent cette impunité.

3 L'anonymat sur Internet

3.1 Les trois principaux types d'anonymat

Trois types d'anonymat principaux ressortent directement lorsqu'il est question d'informatique :

1. *Anonymat via un pseudonyme aux yeux des autres internautes.*
   Utilisé par une écrasante majorité de sites web sur les forums/blogs, celui-ci permet

simplement une reconnaissance de l'internaute au niveau du site. Il est souvent aisé pour l'utilisateur de changer son pseudonyme et d'avoir ainsi l'impression d'acquérir une nouvelle identité aux yeux du monde.

2. *Anonymat au niveau de l'adresse IP.*
   L'adresse IP étant relativement connue des internautes, même des débutants, elle est souvent utilisée par les sites pour reconnaître un même client. Cette adresse étant assignée à chaque connexion internet, on peut remonter à la source relativement facilement, surtout lorsqu'on est un État. Il est devenu toutefois de plus en plus facile de « cacher » son adresse IP via l'intermédiaire de proxy ou de logiciels plus évolués, comme le réseau Tor, mondialement connu et utilisé [16] (voir figure 2). Cette adresse IP se révèle aussi un atout important pour la sécurité des sites web de par sa possibilité à identifier le pays d'origine de l'internaute et ainsi pouvoir bloquer certaines attaques informatiques ou tentatives de voler un mot de passe.
   Bien qu'il soit devenu plus facile de masquer son adresse IP, cet anonymat est souvent superficiel et soumis à de nombreuses contraintes pratiques. Le fait d'utiliser un proxy a souvent tendance à réduire la vitesse de navigation, celui-ci peut aussi décider d'enregistrer tous vos faits et gestes sur les pages vues et il suffit d'une ordonnance d'un tribunal pour que le proxy indique quelle adresse IP originale l'a contacté. Récemment, le célèbre réseau Tor – considéré comme sûr et conseillé pour de nombreux journalistes dans des pays aux régimes totalitaires [33] – a montré sa faiblesse en arrivant à être bloqué par les autorités américaines qui sont arrivées à remonter à la source des créateurs de sites internet de téléchargement illégal et à bloquer divers sites [18]. Avec le nouveau firewall mis en place par la Chine, le pays arrive aussi dorénavant à bloquer les utilisateurs du réseau Tor [21].

3. *Anonymat au niveau de l'adresse MAC.*
   Ce système est bien plus compliqué à mettre en place dans le sens où une personne lambda n'a que rarement entendu parler de l'adresse MAC, voire jamais. L'adresse MAC étant associé à la construction de chaque appareil électronique, elle n'est pas variable comme l'adresse IP pour une machine donnée, et elle est un élément non négligeable pour les autorités et entreprises voulant identifier de manière unique une personne. Cependant, cette adresse n'est pas accessible aux machine étrangères au réseau local de l'utilisateur. Toute personne connectée à ce réseau local a par contre pleinement connaissance de toutes les adresses MAC du réseau. Afin de préserver son anonymat sur un réseau local, il est possible de modifier l'adresse MAC de l'interface réseau utilisée [4].
   Cette limitation au réseau local est cependant de moins en moins d'actualité étant donné qu'une partie de l'adresse IPv6 est générée par défaut à partir de l'adresse MAC de l'interface réseau [17], rendant ainsi possible l'identification d'une machine à partir de n'importe quel nœud de l'internet. Notons que la RFC4941 de l'IETF [17] propose une fonctionnalité d'adresses temporaires régulièrement renouvelées n'utilisant pas l'adresse MAC. Cette fonctionnalité n'est pourtant pas activée par défaut sur les systèmes d'exploitation les plus populaires.

Chacun de ces types d'anonymat est à prendre en compte en fonction des informations que l'on souhaite communiquer sur internet. On peut facilement se rendre compte que l'anonymat n'est déjà plus un « droit par défaut », et que pour ne pas être (facilement) reconnaissable sur le Web il est nécessaire de disposer d'un minimum de connaissances

techniques et être prêt à un certain nombre de concessions.

3.2 Nymwars

Il existe de nombreux exemples d'institutions – politiques ou industrielles – qui tentent d'imposer l'utilisation du véritable nom de l'utilisateur, bannissant les pseudonymes. Ce genre d'affaires s'est forgé un néologisme anglophone : les « *nymwars* », assemblage de « *pseudonym* » et « *wars* », comprenez les « guerres des pseudonymes ».

L'affaire la plus médiatisée de ces dernières années est celle concernant la volonté du réseau social Google+ d'obliger ses utilisateurs à « utiliser le nom par lequel vos amis, votre famille ou vos collègues vous appellent. [10] » Cette politique d'utilisation s'attaquait directement au premier niveau d'anonymat en invoquant qu'ainsi, non seulement le réseau lutterait contre les spams, mais permettrait aussi aux autres utilisateurs de trouver facilement leurs contacts. Non seulement on en devient plus facilement identifiable sur la toile, ce qui ravit les collecteurs d'informations, mais on associe son identité à tout le réseau tentaculaire que représente Google. En effet, un compte Google+ est lié à un agenda, dont nombre de paramètres sont publics par défaut, une adresse email, un compte YouTube et bien d'autres services proposés par la firme. En supprimant un pan de l'anonymat sur leur réseau social, Google propageait donc en réalité cet effondrement à une large gamme de services très utilisés de par sa domination du secteur.

Le tollé ne se fit pas attendre [32] [20], mais il fallut néanmoins trois ans à Google pour faire machine arrière et assouplir sa politique concernant les noms d'utilisateur. Dans un billet publié sur son propre compte Google+ [11], Google annonce mettre fin à cette limitation :

> « Quand nous avons lancé Google+ il y a maintenant plus de trois ans, nous avions imposé nombre de restrictions concernant le nom que vous pouviez utiliser dans votre profil. [...] Aujourd'hui, nous en sommes à la dernière étape : il n'y a plus de restriction concernant le nom que vous pouvez utiliser. » [2]

Si l'opportunité est à présent offerte à tous les utilisateurs de changer leur nom, il ne fait aucun doute que l'écrasante majorité de la communauté Google+ n'en fera rien, reniant tout anonymat et dédouanant Google de ce fait. De plus, quand bien même il est à présent possible de ne plus utiliser son véritable nom, rien ne garantit que Google ne garde pas l'association dans ses bases de données, en faisant profiter ses clients. Nous voyons ainsi que si cette *nymwar* semble terminée, voire même gagnée, c'est encore une fois Google qui a réussi à tirer son épingle du jeu en obtenant le nom et le consentement de millions d'utilisateurs.

Il existe d'autres *nymwars*, comme la politique du « véritable nom » en Corée du Sud en 2008, abandonnée quelques années plus tard suite au vol des identifiants nationaux de millions d'internautes [20], ou encore un ministre allemand[5] ou un sénateur français [27] prônant la disparition des pseudonymes sur l'internet.

4 Les avantages et désavantages de l'anonymat

4.1 Avantages

L'anonymat est sujet d'actualité, mais quels avantages procure-t-il réellement ? Que peut-on répondre à ceux qui ont pour devise *« Je n'ai rien à cacher »* sans davantage d'ar-

2. « When we launched Google+ over three years ago, we had a lot of restrictions on what name you could use on your profile. [...] Today, we are taking the last step : there are no more restrictions on what name you can use. »

guments ? Nous vivons bien sans nous cacher, alors pourquoi nous cacher dans le monde virtuel ?

- *Opposition au gouvernement en place*
  C'est probablement le point le plus important à prendre en compte lorsqu'il s'agit d'estimer l'importance de l'anonymat sur l'internet. On pourrait penser que tant qu'on ne prononce pas de propos diffamatoires, racistes, etc. on peut dire ce que l'on veut dans un pays comme la Belgique. Mais en sera-t-il toujours autant ? Si maintenant l'État promulguait une loi interdisant de critiquer le parti politique en place, que pourrions-nous faire ? Avec l'impossibilité d'exprimer ses opinions politiques sans risquer d'enfreindre la loi, l'anonymat reste la seule solution.

- *Accès à des informations « dangereuses »*
  Cela suit directement le point précédent étant donné que la classification d'information dans la catégorie « dangereuses » est généralement faite par l'État en place. L'exemple de la place Tian'anmen en République Populaire de Chine [1], ainsi que l'accès restreint à l'internet [23] en sont des exemples concrets. En quoi est-ce que se renseigner sur le passé peut-il être considéré comme dangereux, si ce n'est contre le pouvoir en place ? Une des rares façons pour les Chinois de se renseigner sur les exactions commises par le parti unique est de dissimuler leur identité. Les résultats de leurs recherches étant filtrés, les incidents s'étant produits sur la place Tian'anmen tombent peu à peu dans l'oubli [13]. Le droit à l'anonymat serait-il donc le seul rempart face à l'État pour bénéficier du libre accès à la connaissance ?

- *Liberté d'expression*
  Parallèlement à l'accès à certaines informations décrit au point précédent, la liberté d'expression est tout autant un sujet d'actualité lorsque l'anonymat n'est que difficilement accessible sur internet. Étant donné que les messages et autres textes écrits par les internautes chinois sont filtrés sur ordre du gouvernement, et que l'adresse IP permet de facilement retrouver un internaute, ceux-ci doivent trouver d'autres moyens de communiquer.
  Si l'anonymat ne peut être garantit, il subsiste d'autres moyens de protéger ou masquer son contenu, en utilisant par exemple de la stéganographie ou en chiffrant les messages [3].

- *Exprimer des idées contraires à la majorité*
  Pour illustrer ce point, nous pouvons prendre l'exemple – relativement fictif – d'une manifestation du parti socialiste contre le gouvernement libéral en place. Si une personne libérale tentait d'exprimer ses idées à l'intérieur de la manifestation, il y a un risque non nul qu'il soit pris à parti, ou tout du moins remis à sa place. Par contre, si cette même personne venait à discuter sur un forum de discussion dédié au parti socialiste, cette personne serait protégée par son anonymat, si tant est qu'il existe. Il s'agit ici d'un exemple très général, mais on peut illustrer avec d'autres exemples qui sont plus problématiques et se rapportent davantage à l'opinion de la majorité dont il est question. Comment discuter calmement et sans risque de sujets

3. À noter qu'une connexion sécurisée peut donner un faux sentiment de sécurité dans certaines régions, comme en Corée du Nord. Le navigateur web du système d'exploitation officiel du régime n'acceptant que des certificats issus par une autorité du régime, permettant à ce dernier de déchiffrer toutes les communications à la volée. [12]

sensibles tels que l'avortement, le droit au mariage et l'adoption pour les couples homosexuels, le racisme, etc. ? Pour prendre un exemple bien plus extrême, et en le regardant de façon détachée, comment est-ce qu'une organisation suprématiste blanche comme le Ku Klux Klan pourrait exprimer ses opinions sans être traquée par d'autres internautes [31] ? Il n'est pas question ici de défendre un quelconque côté, mais plutôt de montrer que si l'anonymat n'est pas respecté entre internautes, ceux-ci peuvent chercher justice par eux-mêmes.

- *Jugement objectif*
  Les discussions se passant sur l'internet sont souvent sujettes à critiques sur base de l'apparence. Il n'est pas rare de voir des réponses qui sont davantage des insultes et stéréotypes sur base de la couleur de peau, l'âge, le sexe. Ces pensées sont généralement gardées pour soit dans la vie réelle, mais les internautes se sentant intouchables ont beaucoup moins de retenue. Une façon simple de ne pas être discriminé est de cacher son identité lorsque l'on navigue sur l'internet. Cela permet à un individu d'être jugé sur le contenu du message plutôt que sur son identité, pouvant aussi éviter d'être l'objet de persécutions ou de harcèlement.

- *Restriction de l'accès à certains sites*
  Par mesure de sécurité, il arrive que certains sites bloquent l'accès de certains pays à leur site. De nombreuses attaques informatiques venant des États-Unis ou de Chine [26], une solution simple envisagée par certains sites est de bloquer les internautes venant de ce pays [19]. Afin d'accéder à ces sites avec des intentions innocentes, il est nécessaire de changer de forcer son anonymat, notamment en changeant d'adresse IP.

- *Ouverture au dialogue*
  Dans certains pays il n'est pas envisageable de parler de questions telles que l'avortement ou de MST à son entourage étant donné la pression sociale. Il peut aussi se révéler utile de demander des conseils ou un soutien psychologique lorsqu'on est atteint d'une maladie particulièrement difficile à vivre (cancer, VIH, etc.) ou une addiction quelconque (alcool, drogue, etc.). Si il existe bien souvent des structures dans le monde réel pour parler de nos problèmes, elles ne sont pas forcément accessibles à tout le monde, et il peut se révéler bien plus facile de communiquer via internet qu'en personne. Les informations divulguées peuvent se révéler compromettantes [22] si elles atterrissaient dans les mains de recruteurs, de la famille, ou même de spéculateurs. La sécurité devient un point primordial lorsqu'il s'agit de concevoir un système à pareille vocation, mais un système infaillible n'existant pas, l'anonymat reste la meilleure protection, ce qui justifie probablement le succès de sites tels que `doctissimo.fr`.

Nous avons ainsi listé toute une série d'arguments en faveur de l'anonymat sur Internet, et qui montrent bien que le classique « Je n'ai rien à cacher » ne montre qu'une vision pour le moins simpliste du problème. Mais il serait tout aussi ridicule que d'estimer que l'anonymat n'a que des avantages et est à considérer sans aucune réserve.

4.2 Désavantages

Bien qu'il y ait nombre de raisons de rester anonyme sur le web, cela peut aussi engendrer des dérives aux conséquences désastreuses pour des entreprises ou des particuliers.

Certains exemples cités ci-dessous peuvent être considérés comme peu dangereux (restriction de l'accès à certains sites), mais ceux-ci peuvent être détournés à divers usages, comme amener à un accès à l'information/la culture limité à certaines personnes.

- *Escroquerie par mail*
  L'âge d'or des princes nigériens ayant besoin de quelques milliers de dollars pour en débloquer des millions [6] semble être passé. Néanmoins, des personnes se font encore quotidiennement escroquer d'importantes quantités d'argent par des personnes se faisant passer pour des riches personnes cherchant à sortir de l'argent d'un pays lointain. Bien que l'arnaque est facilement reconnaissable, elle fait de nombreuses victimes qui peuvent finir fortement endettées durant leur quête d'obtenir une très importante somme d'argent qui est sensé arrivée au "prochain" paiement de la victime [25]. Si il était possible d'identifier avec certitude l'expéditeur de l'e-mail, il serait sans aucun doute plus facile de réduire le nombre de personnes escroquées.

- *Restriction de l'accès à certains sites*
  Certains service imposent une restriction géographique à leurs utilisateurs pour une simple question de droits de diffusion (YouTube, Dailymotion, les services de rediffusion en ligne des chaînes de télévision, etc.). Les ayant-droits on besoin de localiser l'utilisateur, le dénudant d'une partie de son anonymat. Si l'utilisateur force cet anonymat, par exemple en changeant son adresse IP, il peut accéder à ces services illégalement.

- *Demandes de virements*
  Un autre cas d'escroquerie où l'anonymat entre directement en compte constitue en l'envoi de mails aux services comptables d'une société ou administration publique demandant des virements. Diverses sociétés belges ont été directement concernées par cette fraude où les hackers s'étaient introduits sur les boites mails de dirigeants, avaient imité les mails de demandes de virements classiques en y mettant un de leurs numéros de compte et en l'envoyant au service comptable. On peut voir directement que l'anonymat, ou plutôt le "non-anynomat" imposé par ces adresses mails dont les expéditeurs sont censés être connus, peut se retourner contre n'importe qui lorsque les systèmes de sécurité ne suivent pas. Si une preuve irréfutable de l'envoyeur avait été nécessaire à l'envoi du mail, ou bien si il était possible de retracer les hackers responsables, de nombreux millions n'auraient pu être volés.

La liste pourrait être allongée de façon conséquente : Insultes et cyberharcèlement, usurpation d'identité et manipulation, incitation à la haine et à la violence, pédopornographie, etc.

5 Liste de sujets populaires où l'anonymat est utilisé

Une fois l'anonymat acquis, on peut se demander dans quels domaines il est effectivement utilisés, à quelles fins. Nous avons déjà abordé les avantages et désavantages de l'anonymat sur le web, cette section, quant à elle, se penchera sur l'utilisation qui est faite de cette couverture.

Dans un article publié en 2013 [3], Alex Biryukov *et al.* ont scanné un grand nombre de services proposés sur le réseau Tor, et dans le cas de services HTTP, ont classifié les requêtes de la part des clients.

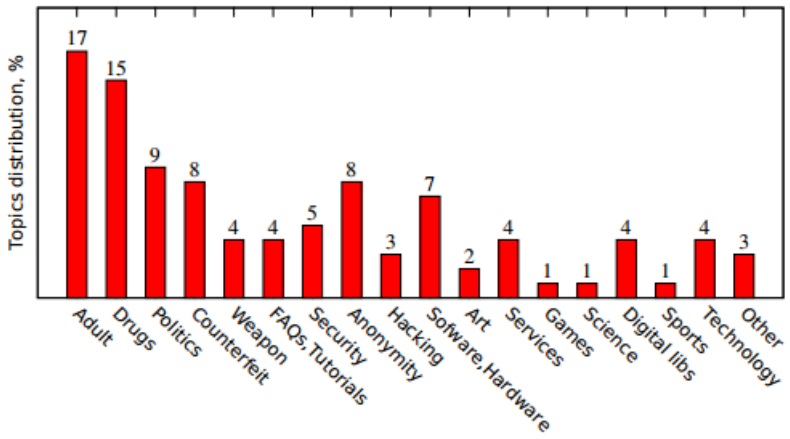


FIGURE 1 – Liste des sujets populaires cherchés sur Tor, 2013 [3]

Comme l'indique la figure 1, le contenu est partagé. On a certes affaire à des contenus illégaux ou pornographiques, mais aussi à une grande partie de requêtes sur la politique ou simplement sur l'anonymat. On est face ici à un débat récurrent quand on aborde l'anonymat : des réseaux tels que Tor ont-ils le droit d'exister, étant le nid de trafics illicites en tous genres ? L'éradication de tels services, afin de soustraire le terreau de cette vilenie, vaut-elle le sacrifice de l'anonymat que d'autres utilisent à bon escient ?

Afin de compléter cette étude, Mark Graham et Stefano De Sabbata ont mis au point une carte (cf. figure 2) représentant l'utilisation du réseau Tor dans le monde. On peut ainsi remarquer que si les États-Unis comptent le plus grand nombre d'utilisateurs, les pays européens et du Moyent-Orient ont une densité d'utilisateurs beaucoup plus importante.

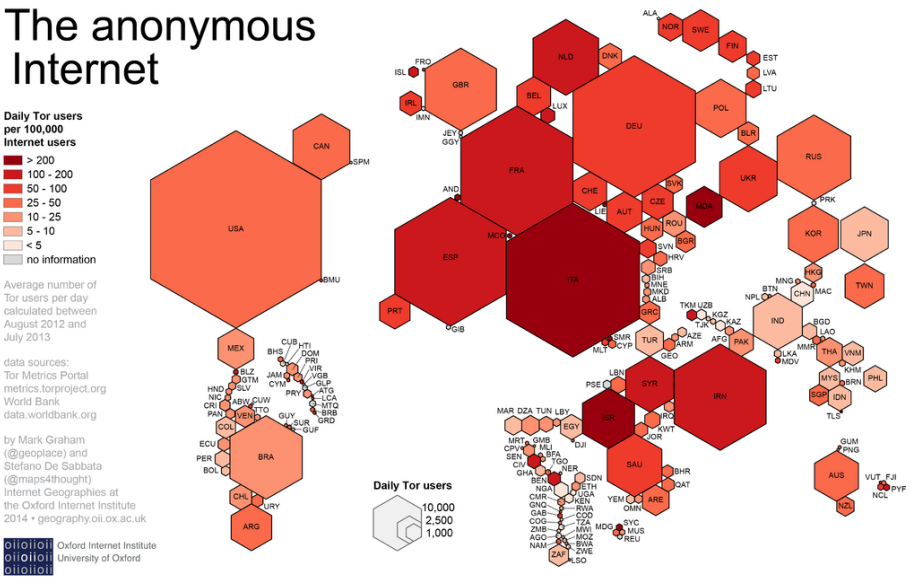


FIGURE 2 – Utilisation du logiciel Tor dans le monde

6 Est-il possible d'être 100 % anonyme sur Internet ?

> *"There is no longer any anonymity on the Web - unless we mandate it. The most personal information about your online habits is collected, bought and sold, often instantaneously and invisibly. Data collection is a business driven by profits at consumers' expense."*
>
> Jackie Speier

Comme mentionné dans la section 3.1, il existe trois niveaux d'anonymat : l'utilisation d'un pseudonyme, l'adresse IP et l'adresse MAC. La plupart des utilisateurs qui surfent sur le web utilisent le premier niveau de l'anonymat, à savoir un pseudonyme quand ceux-ci veulent poster quelque chose anonymement. Bien que cela soit déjà une grande étape vers l'anonymat, car ils seront en effet anonyme aux yeux de la plupart des autres utilisateurs, cela ne les rend pas pour autant complètement anonymes. En effet, lors d'un transfert d'un paquet à travers l'internet, l'adresse IP est attachée à ce paquet comme adresse de retour. Ce paquet va voyager à travers tous les routeurs et serveurs jusqu'à atteindre le serveur où le site web est hébergé, et ceux-ci peuvent garder une copie de l'adresse IP. Le serveur final où est hébergé le site web peut également garder cette adresse IP en mémoire. La question qui se pose alors est : Est-il possible de changer son adresse IP ? La réponse à cette question est oui et non. Oui, on peut la changer en passant par des proxys (i.e. des serveurs intermédiaires) qui remplacent l'adresse IP par la leur, ainsi le site web possédera l'adresse du proxy et non celui de l'utilisateur. Le problème est que cette fois-ci, c'est le proxy qui possède l'adresse IP, ce qui rend juste la réelle adresse IP plus difficile à trouver du point de vue du serveur mais non impossible car il suffit de retracer le proxy. Ce qui amène des gens à utiliser beaucoup de proxys rendant la tâche à identifier un individu beaucoup plus difficile. Non car fondamentalement, on a toujours besoin de savoir où doit aller le paquet, donc l'adresse de retour doit être stocké quelque part. Peu importe la solution adoptée, il faudra toujours faire confiance à un nœud du réseau pour faire la traduction entre le paquet « anonyme » et le véritable utilisateur.

La solution la plus simple, pour un utilisateur qui n'est pas expert en informatique, est d'utiliser un navigateur comme Tor qui rend la reconnaissance extrêmement difficile, en utilisant un circuit virtuel.

En ce qui concerne l'anonymat vis-à-vis des services comme les moteurs de recherche, changer d'IP et supprimer les cookies de sa machine n'est pas toujours suffisant. En de pareil cas, il existe des alternatives offrant un service similaire, mais sans la personnalisation, et donc la publicité, des solutions les plus populaires. Si nous prenons l'exemple de Google, son alternative anonyme est DuckDuckGo, un moteur de recherche qui ne retient aucune information concernant l'utilisateur, et renvoie toujours les mêmes résultats de recherche peu importe l'endroit, ou l'utilisateur faisant la requête.

Le meilleur moyen pour être anonyme à 100 % n'est probablement pas accessible à la majorité des utilisateurs. En plus d'utiliser Tor, on peut également se rendre dans des espaces « open-wifi » où l'adresse IP est donné par cet espace. Il faut également changer son adresse MAC virtuelle car celle-ci peut être vue dans ce réseau wifi, si la configuration du routeur le permet [4].

4. Il est aussi possible d'isoler chaque utilisateur du réseau local sur son propre réseau local virtuel (VLAN), de sorte qu'il ne puisse pas connaître la présence des autres machines sur le réseau.

7 L'anonymat et la vie privée en Belgique

En Belgique, il existe une loi essentielle : « Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel » du 8 décembre 1992. Cette loi définit un cadre du traitement des données des individus en imposant un ensemble de droits et de devoirs à l'individu en question, mais aussi à la personne traitant ces données. Cette loi a été adaptée à de nombreuses reprises, que ce soit avec la loi du 11 décembre 1998 ayant pour but d'adapter des mesures européennes, comme les arrêtés du 13 février 2001 et du 17 février 2003.

Cependant, lorsque l'on s'intéresse à la vie privée sur l'internet, il devient intéressant de se pencher sur la loi « relative aux communications électroniques » du 13 juin 2005, et en particulier sur son arrêté royal du 19 septembre 2013. En effet, ce dernier oblige les opérateurs de télécommunications de conserver une trace de tout le trafic passant sur leur réseau, et ce pour une durée minimale de douze mois. La justice peut alors requérir l'accès à ces données dans le cadre de ses opérations. Si cet arrêté peut sembler mettre les opérateurs dans de beaux draps en les obligeant à conserver les données de navigation de leurs clients, il faut savoir que cette pratique était déjà d'application avant l'application de la directive européenne [2].

8 L'anonymat sur les autres continents

8.1 Europe

> *1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.*
> *2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.*
>
> Article 8 de la Convention Européenne des Droits de l'Homme

> *1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les États de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.*
>
> Article 10 de la Convention Européenne des Droits de l'Homme

La liberté d'expression et le droit à la vie privée sont inscrits dans la Convention Européenne des Droits de l'Homme, cependant l'Union Européenne a aussi émis certaines directives limitant cette même vie privée. L'une d'elles est la directive 2006/24/CE dont nous avons parlé dans la section 7 ; cette dernière demande aux pays membres de conserver les données de leurs citoyens pour une période de six à vingt-quatre mois. Selon un

rapport SECILE [14], seule l'Allemagne n'a pas encore appliquée cette directive à ses lois nationales.

Ce rapport a été publié pour la première fois en novembre 2013, et une seconde fois le 8avril 2014, date à laquelle cette même directive a été invalidée par le Cour de Justice de l'Union européenne [7]. Pourtant, entre 2006 et 2014, 26 pays membres ont modifié leur législation pour intégrer les mesures recommandées par la commission européenne. Maintenant que ces mesures ont été jugées comme étant « une ingérence d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel sans que cette ingérence soit limitée au strict nécessaire. » [7], il semble évident que 26 pays de l'Union Européenne possède une législation s'ingérant dans la vie privée de leurs citoyens, l'invalidation de la directive européenne n'obligeant pas les pays l'ayant appliquée de se rétracter.

Revenons un instant sur les conditions qui ont menées à cette directive : deux attentats meurtriers, l'un le 11 mars 2004 à Madrid et le second le 7 juillet 2005 à Londres. Il est évident que cette directive avait été rédigée dans l'urgence, sous le coup de l'émotion provoquée par ces actes terroristes. Cette directive de 2006 était issue d'une déclaration conjointe de plusieurs pays membres d'avril 2004, soit un mois après l'attentat de Madrid. Il aura fallu huit ans pour que la commission statue de son invalidité. À la lumière de ces informations, quelle directive émergera des attentats de Paris de janvier 2015 ?

8.2 États-Unis d'Amérique

> *"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof ; or abridging the freedom of speech, or of the press ; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."*
>
> Arst Amendment to the United States Constitution

> *"The right of the people to be secure in their persons, houses, papers, and effects* [a]*, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*
>
> *a.* Effects are items of property
>
> 4th Amendment to the United States Constitution

La constitution américaine elle-même garantit la liberté d'expression à ses citoyens, la volonté d'avoir accès à un anonymat sur l'internet est donc d'autant plus forte. Dans certains états, comme en Californie, le droit à l'anonymat a même été établi par décision de justice [28] : « Les citoyens ont la permission d'interagir avec un pseudonyme ou anonymement, tant que ces interactions ne violent pas la loi. » [5] Il existe même des décisions de justice ayant garanti l'anonymat en invoquant le premier amendement [30] [29].

Pourtant, à l'instar de l'Union Européenne, les États-Unis ont adopté des lois potentiellement liberticides et pouvant mettre en péril l'anonymat de leurs citoyens, notamment

5. « People are permitted to interact pseudonymously and anonymously with each other so long as those acts are not in violation of the law »

avec le USA PATRIOT Act, adopté en urgence un mois après les attentats du 11 septembre 2001. En effet, comme le relèvent l'Electronic Frontier Foundation et d'autres organisations, cette loi donne un certains nombre de pouvoirs aux autorités d'investigation qui sont potentiellement en contradiction avec certains amendement de la constitution, notamment le quatrième.

9 Conclusion

> *"Human beings are not meant to lose their anonymity and privacy."*
>
> Sarah Chalke

Au vu de tous ces arguments, l'utilité de l'anonymat ne fait plus aucun doute. Elle permet à un individu de s'exprimer librement tout en protégeant l'identité de celui-ci, ce qui permet au final de protéger sa vie privée.

Si l'anonymat n'existait pas, les gens feraient plus attention à ce qu'ils écriraient sur le web par peur de représailles physiques, verbales, morales ou même légales. Des événements récents, tels que l'attaque de Charlie Hebdo, nous montrent ce qu'il peut se passer quand des gens n'acceptent pas que d'autres personnes s'expriment librement.

Si l'anonymat n'existait pas, nombre de personnes se retrouveraient seules face à leurs problèmes, n'osant pas en discuter à visage découvert. Si l'anonymat n'existait pas, c'est tout un pan de la connaissance et de l'information qui serait inaccessible aux citoyens des régimes les plus répressifs. Si l'anonymat n'existait pas, ce seraient ces même citoyens qui ne pourraient communiquer sur leur situation avec le reste du monde.

Pour conclure, nous pouvons dire et même affirmer que l'anonymat sur l'internet est plus un bien qu'un mal, et doit être protégé tout autant que la liberté d'expression. À vrai dire, et si l'on y réfléchit bien, l'anonymat protège la liberté d'expression, en protégeant l'identité et la vie privée de celui qui s'exprime. Bien qu'il existe certes des désavantages à l'anonymat, chaque personne devrait avoir le choix de s'exprimer anonymement ou non.

Références

[1] Arte. Les manifestations de tiananmen, inconnues en chine. http://info.arte.tv/fr/les-manifestations-de-tiananmen-inconnues-en-chine, juin 2014. Consulté le 13 janvier 2015.

[2] Belga. Stockage des données : Vande lanotte rassure, l'opposition s'inquiète. *La Libre*, septembre 2013. http://www.lalibre.be/actu/belgique/stockage-des-donnees-vande-lanotte-rassure-l-opposition-s-inquiete-51dc427b3570600385670b4e.

[3] Alex Biryukov, Ivan Pustogarov, and Ralf-Philipp Weinmann. Content and popularity analysis of tor hidden services. *CoRR*, abs/1308.6768, 2013.

[4] Edgar D. Cardenas. Mac spoofing - an introduction. http://www.giac.org/paper/gsec/3199/mac-spoofing-an-introduction/105315, août 2003. Consulté le 13 janvier 2015.

[5] Richard Connor. German minister urges end to web anonymity after norway attacks. *Deutsche Weller*, août 2011. http://www.dw.de/german-minister-urges-end-to-web-anonymity-after-norway-attacks/a-15301860.

[6] Andrew Couts. The nigerian prince in your inbox has been around for over 500 years. décembre 2012. http://www.digitaltrends.com/web/the-first-nigerian-prince-scam/.

[7] Cour de justice de l'Union européenne. Communique de presse no 54/14. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054fr.pdf, avril 2014. « La Cour de justice déclare la directive sur la conservation des données invalide ».

[8] Cour de justice de l'Union européenne. La Cour de justice déclare la directive sur la conservation des données invalide. Communiqué de presse no 54/14, avril 2014.

[9] Facebook. Company Info – Statistics : « 1.35 billion monthly active users as of September 30, 2014 ». http://newsroom.fb.com/company-info/, janvier 2015. Consulté le 14 janvier 2015.

[10] Google. Google+ Policies & Principles. http://www.google.com/intl/en/+/policy/content.html, 2011. Mis à jour depuis juillet 2014. Le texte original, en juillet 2011, était le suivant : « To help fight spam and prevent fake profiles, use the name your friends, family or co-workers usually call you. ».

[11] Google+. Google+ status. https://plus.google.com/+googleplus/posts/V5XkYQYYJqy, juillet 2014. Consulté le 09 décembre 2014.

[12] Robert Hansen. North Korea's Naenara Web Browser : It's Weirder Than We Thought. https://blog.whitehatsec.com/north-koreas-naenara-web-browser-its-weirder-than-we-thought/, janvier 2015. Consulté le 10 janvier 2015.

[13] Here and Now. How the tiananmen square massacre has been largely forgotten. http://hereandnow.wbur.org/2014/06/04/tiananmen-louisa-lim, juin 2014. Consulté le 13 janvier 2015.

[14] Chris Jones and Ben Hayes. The EU Data Retention Directive : a case study in the legitimacy and effectiveness of EU counter-terrorism policy. Technical report, SECILE – Securing Europe through Counter-Terrorism : Impact, Legitimacy & Effectiveness, avril 2014.

[15] Justin Kruger and David Dunning. Unskilled and unaware of it : how difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of Personality and Social Psychology*, 77(6) :1121 – 1134, 1999.

[16] Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker. Shining light in dark places : Understanding the tor network. `http://cs.gmu.edu/~mccoy/papers/PETS2008_37.pdf`, 2008. Consulté le 13 janvier 2015.

[17] T. Narten, R. Draves, and S. Krishnan. RFC 4941 : Privacy Extensions for Stateless Address Autoconfiguration in IPv6. Technical report, The IETF Trust, septembre 2007.

[18] U.S. Department of Justice. More than 400 .onion addresses, including dozens of 'dark market' sites, targeted as part of global enforcement action on tor network. `http://www.fbi.gov/news/pressrel/press-releases/more-than-400-.onion-addresses-including-dozens-of-dark-market-sites-targeted-as-part-of-global-enforcement-action-on-tor-network`, novembre 2014. Consulté le 13 janvier 2015.

[19] Keith Parkansky. Stop traffic from china ip addresses to protect your web server from chinese hackers. `http://www.parkansky.com/china.htm`.

[20] Eric Pfanner. Naming names on the internet. *The New York Times*, septembre 2011. `http://www.nytimes.com/2011/09/05/technology/naming-names-on-the-internet.html`.

[21] MIT Technology Review. How china blocks the tor anonymity network. `http://www.technologyreview.com/view/427413/how-china-blocks-the-tor-anonymity-network/`, avril 2012. Consulté le 13 janvier 2015.

[22] RTBF. Piratage chez mensura : les hackers ont publié les données confidentielles. novembre 2014. `http://www.rtbf.be/info/societe/detail_chantage-a-mensura-les-hackers-ont-publie-les-donnees-confidentielles?id=8421603`.

[23] Reporters sans frontières. Chine. `http://surveillance.rsf.org/chine/`. Consulté le 13 janvier 2015.

[24] Bruce Schneier. Attacking tor : how the nsa targets users' online anonymity. *The Guardian*, octobre 2013. `http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity`.

[25] Anna Song. Woman out 400k to 'nigerian scam' con artists. novembre 2008. `http://www.katu.com/news/local/34292654.html`.

[26] IAN STEADMAN. Reports find china still largest source of hacking and cyber attacks. avril 2013. `http://www.wired.co.uk/news/archive/2013-04/24/akamai-state-of-the-internet`.

[27] Xavier Ternisien. Un blogueur doit-il rester anonyme ? *Le Monde*, mai 2011.

[28] United States District Court for the Northern District of California. Columbia Insurance Company v. Seescandy.com, et al. `http://cyber.law.harvard.edu/property00/domain/Sees.html`, mars 1999.

[29] U.S. Supreme Court. Talley v. California. 362 U.S. 60, 1960.

[30] U.S. Supreme Court. Buckley v. American Constitutional Law Foundation, Inc. 525 U.S. 182, 1999.

[31] Julien Vlass. Opkkk : quand anonymous pirate le ku klux klan et l'humilie sur la toile. novembre 2014. http://www.rtbf.be/info/medias/detail_opkkk-quand-anonymous-pirate-le-ku-klux-klan-et-l-humilie-sur-la-toile?id=8403473.

[32] Jillian York. A case for pseudonyms. *Electronic Frontier Fondation*, 2014. https://www.eff.org/deeplinks/2011/07/case-pseudonyms.

[33] Ethan Zuckerman. Comment blogger de manière anonyme. http://fr.rsf.org/comment-blogger-de-maniere-anonyme-14-09-2005,14980.html, avril 2009. Consulté le 13 janvier 2015.