[Fiche 10] L'anonymat sur Internet

"*Sur Internet, personne ne sait que vous êtes un chien*". Cet ancien adage d'Internet était peut-être pertinent en 1993, actuellement la situation est plus complexe. S'il reste possible d'utiliser un pseudo séparé de nos autres identités pour discuter ou commenter et choisir son identité selon le contexte, on n'est pas pour autant anonyme. Quand on navigue sur Internet, on laisse un grand nombre de traces. Parmi elles, l'adresse IP de l'ordinateur et d'autres informations qui permettent d'être identifié.

Ainsi, par défaut, chaque accès à des services sur Internet est enregistré ("*loggé*") par différents acteurs (fournisseurs d'accès Internet, services auxquels on se connecte, éventuels acteurs intermédiaires...). Le fournisseur d'accès disposant normalement de l'identité civile de la personne titulaire de la connexion, il peut (et y est contraint dans certains cas) la livrer à une autorité accompagnées des différentes données de connexion (metadonnées) dont il dispose. Tout ordinateur transmet aussi automatiquement à tous les services en ligne un certain nombre d'informations (dont le *user-agent* qui correspondent aux données transmises par le navigateur indiquant le système d'exploitation, le navigateur, etc.) qui peuvent permettre de l'identifier.

Pourtant, bien que la possibilité d'une forme d'anonymat puisse engendrer des problèmes (commentaires malveillants, insultes ou menaces, etc.), ce peut être le seul rempart contre des sanctions injustes pour avoir exprimé une opinion différente ou s'être renseigné sur des sujets sensibles. Il existe de très nombreuses raisons légitimes pour ne pas souhaiter que ses navigations sur Internet soient reliées à son identité civile : protection contre une surveillance abusive (qu'elle soit privée ou publique), échanges protégés dans le cadre de professions ou activités sensibles (avocat·e, journaliste, militant·e, lanceu·se d'alerte)... et ne serait-ce que la volonté de ne pas être perpétuellement suivi·e et épié·e.

Des outils existent pour protéger ses identités et participer ainsi à renforcer la liberté d'expression et d'opinion. Le principe est de faire transiter ses communications de façon sécurisée par un autre serveur qui accédera à notre place aux contenus désirés. On empêche ainsi le service final ou tout autre intermédiaire de connaitre la provenance de la connexion.

C'est notamment le fonctionnement d'un proxy ou d'un Réseau privé virtuel (ou *VPN*), mais c'est aussi le principe de base d'un réseau comme "TOR" destiné à protéger les communications.

Usage du réseau Tor

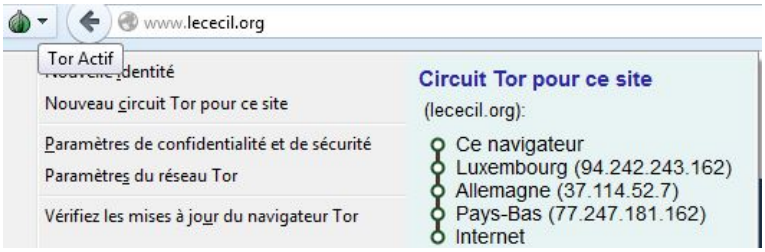
Qui s'intéresse un peu à la protection de la vie privée sur Internet a sans doute déjà entendu l'acronyme "TOR" sans pour autant forcément savoir ce dont il s'agit.

En pratique, Tor (*The Onion Router*, le "routage en oignon") est un réseau informatique qui s'appuie sur de nombreux routeurs, appareils et serveurs qui vont assurer automatiquement la redirection des "paquets de données", donc des communications sur Internet. La multiplicité de ces routeurs, servant de couches de protection, rend extrêmement difficile de retracer leur provenance. Pour cette raison, il est souvent critiqué par les autorités et services policiers.

Il est développé par le "projet Tor" qui a pour objectif :
"*d'améliorer les droits de l'homme et les libertés fondamentales en créant et déployant des techniques libres et ouvertes protégeant l'anonymat et la vie privée, en soutenant leur usage et leur disponibilité inconditionnelle et en encourageant leur compréhension scientifique et populaire*" (traduction CECIL).

Son objectif principal est de protéger l'origine d'une connexion sur Internet et donc de favoriser l'anonymisation des communications sur Internet. Ainsi, une requête à un serveur va transiter par de nombreux ordinateurs ou serveurs répartis dans le monde empêchant normalement l'hébergeur final ou à une organisation surveillant un point précis du réseau (telle que la *NSA*) de savoir qui est l'auteur de cette requête. Pour simplifier un peu, au lieu de l'adresse IP de l'auteur de la requête, c'est celle d'un nœud réseau Tor qui sera détectée rendant l'identification ou toute tentative de traçage extrêmement difficile.

À titre d'exemple, un circuit Tor classique pour accéder à un site ressemblera à cela :



Pourquoi utiliser Tor ?

Ainsi, Tor complique considérablement la tâche pour identifier qui accède à quoi, qui recherche quoi, qui transmet quoi à qui, etc. Même les sites consultés sont incapables d'identifier le véritable auteur de la requête.

Cela peut s'avérer nécessaire et être ainsi utile à :

- toute personne pour préserver sa vie privée et son intimité ;
- tout·e professionnel·le pour favoriser la confidentialité d'échanges d'informations ;
- des lanceu·ses d'alertes et des journalistes pour se protéger et informer depuis des zones dangereuses, sans risques de censure par

certains pays ou opérateurs ;
- éviter d'être identifié dans des pays peu démocratiques et potentiellement torturé ou tué pour ses connexions en ligne ;
- des militaires pour garantir l'intégrité de l'information ;
- contourner des formes de censure ou de territorialisation des informations ;
- etc.

Même si on se soucie peu de protéger sa vie privée, utiliser Tor sans réel besoin d'anonymat, protège indirectement celles et ceux qui l'utilisent par nécessité en faisant ainsi grossir "la botte de foin" : en évitant que leurs communications sortent du lot.

Comment utiliser Tor ?

La croyance commune est qu'il est difficile d'utiliser Tor, qu'il s'agit d'une pratique de spécialiste... ce n'est pas le cas. Utiliser Tor c'est aussi simple qu'utiliser n'importe quel navigateur.

> Il suffit de télécharger le navigateur Tor, *Tor Browser*, qui est disponible pour tous les systèmes d'exploitation et de l'installer sur son ordinateur ou même sur une clef USB.

À partir de là on peut naviguer sur Internet *via* le réseau Tor sans autre opération !

> Sur la page d'accueil, cliquer sur "Tester les paramètres du réseau Tor" pour vérifier que tout est fonctionnel.

C'est donc loin d'être une opération de spécialiste : c'est accessible à tou·tes ! Une autre croyance courante est celle de la lenteur problématique du réseau TOR. Si cela était pour partie vrai il y a quelques années, grâce à de nombreux acteurs (tels que l'association Nos oignons en France) le réseau reste suffisamment fluide pour un usage basique d'Internet !

Les limites

Même si aucun élément ne permet de penser que la sécurité de Tor soit actuellement compromise (voir les liens présentés en fin de fiche), le réseau n'offre pas pour autant une garantie absolue d'anonymat, mais, bien utilisé, une amélioration substantielle de la protection de l'origine des communications. Au-delà de failles pouvant être découvertes dans le futur, certaines mauvaises pratiques peuvent toutefois révéler une identité par :

- la transmission d'informations, personnelles ou non lors des navigations (utilisation du même pseudo ou mot de passe, syntaxe similaire...) ;
- l'utilisation de modules ajoutés ou de logiciels tiers (flash, java, extensions de navigateur...) ;
- l'ouverture de documents téléchargés *via* le *Tor Browser*, en étant encore connecté qui peuvent accéder à des documents sur le réseau (et ainsi transmettre la véritable adresse IP et données d'identification).

Enfin, si on utilise Tor pour communiquer directement avec d'autres personnes, d'autres précautions sont nécessaires pour protéger son identité et ses communications.

Utiliser Tor ne permet donc pas de tout faire si l'on souhaite protéger fortement son anonymat et n'est pas adapté à tous les types d'utilisation : pas de contenus "flash", pas de téléchargement massif ni "pair à pair", des limites possibles sur les flux vidéos, une absence d'identification durable sur les sites consultés (mais c'est le but), une personnalisation des sites (langage, etc.) dépendante du dernier nœud réseau avant la requête, etc.

Il faut noter que si le dernier nœud par lequel les communications transitent est malicieux, il pourra intercepter l'intégralité du trafic si la communication n'est pas chiffrée. Il faut donc être très prudent en ne transmettant *via* Tor que des informations chiffrées (par le *HTTPs*). Il faut toutefois relever qu'une chercheuse en sécurité a utilisé une méthodologie pour déterminer l'existence de serveurs Tor malicieux et dans son étude, seules 6 sorties Tor sur 1500 se sont révélées problématiques.

De plus, si quelqu'un·e est ciblé·e directement par une surveillance de son réseau local ou de son ordinateur (infecté par un virus par exemple) l·a surveillant·e connaitra toutes ses communications.

Les "services cachés"

Le réseau Tor permet d'accéder aux différentes pages Web. Mais en plus, les différents routeurs et serveurs qui permettent de naviguer *via* Tor peuvent aussi venir héberger des pages et des services de messagerie instantanée. Cet hébergement est protégé par le réseau Tor et uniquement accessible par ce biais, il n'est guère possible d'identifier le propriétaire. Cette fiche n'a pas pour objet de détailler comment héberger de telles pages qui vont être identifiées par une adresse finissant en .onion, mais il est possible de le trouver sur la page du projet Tor.

Si des pages peu respectueuses des lois françaises sont accessibles par de telles adresses (exemple : *"The Silk Road"*), en même temps cela permet également à des dissident·es politiques de pays peu démocratiques d'échanger et de transmettre des informations.

À titre d'exemple, une fois le *Tor Browser* lancé, essayer :

- 3g2upl4pq6kufc4m.onion/ qui renvoie vers DuckduckGo sur Tor ;
- torlinkbgs6aabns.onion/, ou zqktlwi4fecvo6ri.onion/ qui sont des listes de liens ".onion" que l'on peut trouver dans ces services cachés.

Les autres réseaux anonymisants

Il existe d'autres initiatives similaires à Tor qui disposent d'autres atouts ; elles offrent aussi des bonnes garanties d'anonymat et peuvent même avoir un intérêt supérieur à Tor, mais elles n'ont pas le même degré d'aboutissement ou de qualité de service. Le CECIL propose toutefois de découvrir :

- I2P pour "*Invisible Internet Project*", qui combine un fonctionnement proche de Tor et une approche en "pair-à-pair". Il permet ainsi le téléchargement de fichiers et l'établissement de communications anonymes. Grâce à I2P deux ordinateurs peuvent communiquer entre eux (*via* des intermédiaires), plus simplement que sur Tor, sans que l'un puisse identifier l'adresse IP de l'autre.
- Freenet, qui fournit des services similaires, mais est plutôt axé sur la publication de documents décentralisés ; ainsi si une personne met un document sur Freenet celui-ci va se retrouver hébergé, découpé en différents morceaux, sur de nombreux serveurs et ne pourra plus être supprimé tant que le réseau existe et ce même si l'auteur y était contraint.

Ces deux services ne nécessitent que d'installer un logiciel pour les essayer et se faire sa propre opinion.

Usage d'un VPN

Acronyme anglais de "réseau privé virtuel", un VPN (*Virtual Private Network*) est une technique permettant de créer un lien réseau direct, un "tunnel" entre deux ordinateurs éloignés. Ainsi quand un ordinateur est connecté à un VPN, il peut accéder au réseau "au travers" d'un autre, qui, aux yeux du réseau, sera celui qui réalise les opérations. Cela permet par exemple de se connecter à distance au réseau interne (*intranet*) d'une entreprise, mais aussi d'accéder à Internet sans que l'adresse IP de la personne qui utilise le VPN soit enregistrée. Seules l'adresse IP et les caractéristiques techniques du serveur offrant le VPN circuleront sur le réseau.

Des entreprises proposent des solutions de VPN qui vont protéger la confidentialité de l'origine des communications. En souscrivant à leurs services, si la communication en direction du VPN est sécurisée (chiffrement...), il sera très difficile de déterminer qui a accédé à tel ou tel contenu sur Internet, les informations d'identification transmises étant celles du VPN de l'entreprise.

Le niveau de sécurisation est fonction de l'entreprise. Il faut donc qu'elle présente certaines garanties. Tout dépend des besoins. Ainsi, si le seul objectif est d'éviter que les services utilisés puissent "profiler" l'adresse IP, la plupart des solutions existantes sont convenables.

Dans l'hypothèse d'un service qui utilise l'adresse IP pour localiser l'internaute, par exemple certaines vidéos dont l'accès est restreint aux résidents d'un pays, l'usage d'un VPN localisé dans ce pays peut permettre de se soustraire à cette contrainte.

S'il y a absolument besoin qu'une communication ne soit pas tracée jusqu'à son émetteur par les autorités, l'immense majorité des VPN ne seront pas adaptés. En effet, ces entreprises restent soumises aux lois nationales. Elles doivent respecter les mandats judiciaires de transmissions de données d'identification. Les garanties de confidentialité offertes par un VPN sont dépendantes non seulement de la localisation de l'entreprise et de ses serveurs, mais aussi de ses conditions contractuelles et de sa bonne volonté à coopérer avec les autorités publiques. Face à ce risque de surveillance, le CECIL ne saurait faire une recommandation précise (sans possibilité d'auditer véritablement ces services ni de tester toutes les solutions).

Il existe de très nombreux services et comparatifs de services. Offrir un tel service a un coût, il faut donc se méfier des services "gratuits", dont la rémunération est indirecte (publicité, produit d'appel, utilisation des données à d'autres fins...). Il existe toutefois quelques services gratuits aux caractéristiques limitées (en bande passante, en débit général, en protocoles disponibles...) qui apparaissent comme fiables si l'objectif est seulement de se protéger des entreprises commerciales. On peut aussi citer des VPNs issus d'organisations sans but lucratif ayant pour vocation de protéger la vie privée :

- Arethusa limité toutefois à la seule navigation web dans sa version gratuite ;
- Autistici, au débit toutefois très limité ;
- RiseUp, accessible sur seule cooptation ou acceptation sur demande.

Pour les solutions payantes plus complètes, sans pouvoir faire de recommandations précises voici les points qu'il est important de prendre en compte :

- les garanties techniques : stabilité de l'infrastructure, du service, nombre de serveurs et répartition sur le globe, etc. ;
- les logiciels et protocoles utilisés, il faut ainsi s'assurer qu'il s'agisse d'un logiciel fiable, principalement "OpenVPN", sous licence libre et qui semble faire ses preuves en termes de sécurité ;
- la localisation juridique de l'entreprise et de ses serveurs qui conditionne la législation à laquelle elle est soumise et donc aux potentielles demandes des États concernés ;
- les garanties juridiques en termes de vie privée présentes dans les conditions commerciales.

Il faut bien prendre le temps d'analyser le service et d'en connaître les limites, un VPN sérieux protégera contre la surveillance privée et évitera les méthodes liées à la seule surveillance du réseau (*IP-tracking*, limites liées à la localisation de l'adresse IP, surveillance automatique des connexions de "pair à pair"...), mais ne constituera pas une garantie absolue contre des demandes étatiques ou judiciaires d'identification de connexion.

Pour aller plus loin :

Sur Tor

- Le site officiel de Torproject.org
- Télécharger le *Tor Browser* (ou navigateur Tor)
- Une description exhaustive des usages légitimes de Tor torproject.org/about/torusers.html (en anglais)
- Il est possible de se protéger d'une compromission de son ordinateur en utilisant Tor *via* le système d'exploitation Tails utilisé en Live-Usb.
- Pour soutenir le développement de nœuds Tor et ainsi renforcer le réseau, il est possible en France de participer à l'association "Nos Oignons"
- Une vidéo de présentation de Tor (sur Youtube), Navigation anonyme avec Tor Browser - TechTour : Démo
- A. Guiton, Liberation.fr, Tor : Mails-toi de tes oignons
- Lundi.am, Utiliser Tor contre la Loi Renseignement ? Réponses avec Lunar, membre du projet Tor
- The Guardian (en anglais), NSA and GCHQ target Tor network that protects anonymity of web users, s'appuyant sur des documents dévoilés par E. Snowden témoignant que si la NSA souhaiterait pouvoir "désanonymiser" les communications du réseau Tor, jusqu'ici elle semble ne pas y être parvenue. Les documents dévoilés de l'entreprise *The Hacking Team* témoignent du même état de fait
- J. Bearman, sur Wired (en anglais), The Untold Story of Silk Road, un récit captivant en 2 parties conséquentes retraçant l'histoire du site *The Silk Road* et de son supposé créateur Ross Ulbricht alias *Dread Pirate Robert*
- lemagtechno.com, Réseau anonyme lequel choisir, un rapide comparatif (en français) de I2P, Tor et Freenet de ces trois services.

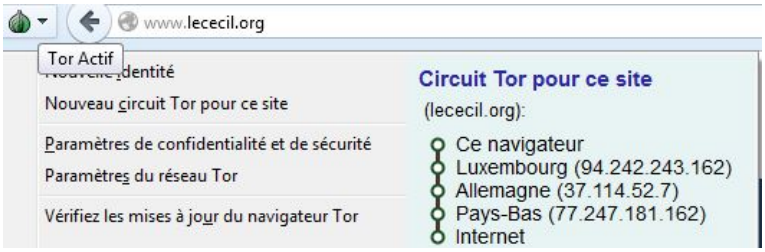
Sur les VPN

- Vpnblog.net dispose de nombreux comparatifs et analyses sur les VPN qui semblent fiables, attention toutefois de nombreuses comparaisons de VPN sont uniquement promotionnelles et loin d'être objectives.
- Une analyse un peu ancienne (2011) des garanties concernant la vie privée de nombreux VPN chez Torrent Freak, traduite par Torrent News en français, Quels fournisseurs de VPN prennent vraiment l'anonymat au sérieux ?
- Parmi les VPN payants les plus communément cités comme techniquement fiables (pas forcément juridiquement) on trouve notamment IPVanish.com, localisé aux États-Unis, qui revendique ne pas conserver de logs, on peut aussi citer le français Toonux.net engagé dans la protection de la vie privée, mais aux possibilités techniques plus limitées (pas de choix de pays de sortie par exemple) ou Ipredator.se, une solution VPN co-fondé par Peter Sunde un des fondateurs de The PirateBay.
- L. Adam, ZDnet.fr, Controverse autour de la sécurité des VPN grand public, suite à une étude critiquant la sécurité des principaux VPN payants
- Attention, une faille dans un des protocoles de communication (WebRTC) a été découverte début 2015 et peut dévoiler l'identité de l'utilisateur d'un VPN. Les indications pour s'en défaire son disponible sur Numerama, Vous utilisez un VPN ? Une faille dévoile votre adresse IP réelle
- Desgeeksetdeslettres.com, La différence entre un proxy et un VPN, qui revient aussi sur les limites des deux outils

Plus d'information sur l'anonymisation en général :

- Un excellent article de The Intercept (en anglais), Chatting in Secret While We're All Being Watched, qui combine à la fois les explications sociétales sur les "besoins" de communiquer anonymement et des explications pratiques sur "comment" par le biais du chiffrement et de l'usage du réseau TOR
- Une rapide présentation sur itpro.co.uk (en anglais), **Security researchers develop anonymous web browsing**, d'un projet de recherche d'une solution similaire à Tor pour garantir l'anonymat sur Internet
- Un article de GoldenFrog.com une entreprise proposant des solutions commerciales, **Myths about VPN logging and anonymity**. L'article est très partial, mais présente bien les limites de la recherche de confidentialité / d'anonymat et les fausses promesses à ce niveau

Fiche 10 [publiée le 6 novembre 2015, dernière mise à jour avril 2018]



Félicitations. Ce navigateur est configuré pour utiliser Tor.

Votre adresse IP semble être : **176.10.99.200**