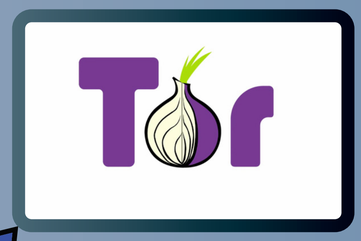
# Internet : Anonymat ou pseudo-nymat ?






## Les Métadonnées

Elles désignent les données qui parlent des données.
Elles sont souvent intégrées dans les données elles-mêmes.
Cela peut concerner : les noms des interlocuteurs lors d'un appel, la catégorie d'un produit lors d'un achat....

### Pourquoi sont-elles importantes pour notre anonymat ?

- Elles savent bien se cacher. Par exemple, peu de personnes savent que les photos qu'ils prennent avec leur téléphone sont souvent accompagnées de métadonnées

- Elles s'exploitent facilement, principalement car elles sont en général clairement définies ! Cela fait qu'elles sont devenues une cible évidente, avec la démocratisation des techniques cryptographiques et les changements législatifs.

## Le Stockage

des informations de chaque utilisateur grâce à :

- **L'adresse IP** (Internet Protocol), un numéro d'identification qui est attribué de façon permanente ou provisoire à chaque appareil connecté à un réseau utilisant ce protocole. Elle est donc en quelque sorte la plaque d'immatriculation de notre ordinateur lorsque nous sommes connectés à l'internet.

- **L'identification** sur des sites : Lorsque nous nous identifions sur un site quelconque (réseau social, messagerie..) nous ne sommes pas anonymes car nous donnons notre adresse e-mail ainsi qu'un mot de passe qui est en général universel pour tous nos comptes .

De plus, des données sont aussi très certaine-ment collectées à notre insu lors de nos consultations web grâce aux cookies, relatant de nos moindres faits et gestes sur Internet.

## Les Applications

- **Tor** est un réseau informatique superposé mondial et décentralisé. Il se compose d'un très grand nombre de serveurs par lesquels transitent les requêtes d'un utilisateur. Le passage de la même requête par plusieurs serveurs ou noeuds permet de brouiller les pistes et d'empêcher de déterminer qui est à l'origine de celle-ci. Cependant, comme tout système, il a des failles.

- Les **Backdoors**, les « portes de secours » laissées par les développeurs de programmes (ou par des tiers), qui permettent de surveiller l'activité des logiciels et même d'en prendre le contrôle. Celles-ci peuvent ensuite être utilisées, par des hackers, pour récupérer des informations ou par exemple propager un virus via les droits d'administration que le logiciel détient, ou par des développeurs pour endiguer une attaque cybercriminelle sur un réseau.

## La Société

- **Récemment,** Internet a été accusé d'être une plateforme d'organisation pour différents cybercriminels et/ou terroristes, sous couvert de l'anonymat que peut procurer le Web Pour faire face à cela, la

**Loi sur le Renseignement**

a été promulguée le 24 Juillet 2015 afin que l'Etat puisse accéder aux données privées de n'importe quel citoyen.
Cette Loi est très controversée car elle constitue une véritable violation de la vie privée et des droits de l'Homme.
Il est donc légitime de se poser la question de savoir si cette loi contribue à notre sécurité ou si au final elle permet à l'Etat de déséquilibrer la «neutralité du net», très importante pour la liberté d'expression.

## Julien Assange

Vous connaissez sûrement ce personnage ou bien du moins sa fameuse démarche avec la création de son site web "WikiLeaks" en 2006. Dans le but de dévoiler des informations ainsi que des analyses politiques et sociales partout dans le monde, sa raison d'être est de donner une audience aux lanceurs d'alertes et aux fuites d'information. Cependant, se serait-il mis autant en danger s'il l'avait fait de manière anonyme ? L'anonymat sur internet aurait-il vraiment pu protéger quelqu'un qui a publié plusieurs millions de documents relatifs à des scandales de corruption, d'espionnage et de violations de droits de l'homme concernant des dizaines de pays dans le monde ?


LI Clément - DARGEIN Christian - ALI BARREH Amareh - MANNEVY Kostia - TEBOUL DAN

IUT Lyon 1
l'excellence technologique

Département Informatique - IUT Lyon 1