

PROTECTION DE LA VIE PRIVÉE

Contre la surveillance de masse.

A decorative graphic consisting of several parallel white lines of varying lengths, slanted upwards from left to right, located in the bottom right corner of the image.

Protection de la vie privée sur internet.

Internet est gratuit, c'est vous le produit!

« Ce n'est pas le boulot des consommateurs de savoir ce qu'ils veulent. (Steve Jobs - Apple) ».

Cette phrase indique bien les buts des GAFAM et des services de surveillance électronique qui enregistrent toutes nos informations pour dresser notre profil type.

Ces informations vendues ensuite à des publicitaires nous incitent à acheter des produits dont nous n'avons pas forcément besoin.

Je vous donnerais des pistes pour vous protéger de la surveillance de masse sur internet.

Vous découvrirez également l'inventaire des différents réseaux internet. (P2P), (DEEP WEB), (DARK WEB).

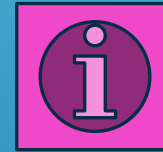
Les capteurs d'un smartphone et leurs utilisations

Tous Les capteurs d'un smartphone et leurs utilisations:

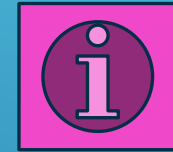
Caméra 1 (arrière)	⇒ Photo, vidéo, lecteur flashcode, loupe, scanner, mesures, Réalité Augmentée.
Caméra 2 (avant)	⇒ Auto-photos (selfies), visiophonie, webcam.
Écran tactile	⇒ Clavier, dessin, jeux.
Microphones de (1 à 3*)	⇒ Téléphone, dictaphone, vidéo, reconnaissance vocale, reconnaissance de musiques.
Détecteur de proximité	⇒ Désactive l'écran tactile près de l'oreille en communication téléphonique.
Capteur de luminosité	⇒ Adaptation de la luminosité à l'éclairage ambiant.
Capteur effet hall	⇒ Détecte la fermeture ouverture de l'étui.
Magnétomètre 3 axes donc 3 capteurs	⇒ Boussole, guidage GPS, détecteur de métaux, Réalité Augmentée.
Gyromètre (gyroscope) 3 axes donc 3 capteurs	⇒ Jeux, localisation, Réalité Augmentée.
Accéléromètre 3 axes donc 3 capteurs	⇒ Jeux, orientation smartphone, niveau, Réalité Augmentée, stabilisation d'image.
Thermomètre #	⇒ Mesure température.
Hygromètre #	⇒ Mesure humidité.
Capteur de geste infrarouge #	⇒ Détecte le Mouvement de la main.
Capteur de pression #	⇒ Baromètre, altimètre.
Scanner d'empreintes digitales #	⇒ Identification de l'utilisateur.
Capteur d'impulsions cardiaques #	⇒ Mesure la fréquence cardiaque.

= dans smartphone ou tablette haut de gamme

Antennes	et circuits de réceptions:
GPS	⇒ Géolocalisation, guidage GPS
2G,3G, 4G, 4G+	⇒ Téléphone, accès internet (qq km)
Wi-Fi	⇒ Communication moyenne distance (20 m), internet, imprimante
Bluetooth	⇒ Communication courte distance (qq m), oreillette, imprimante.
NFC	⇒ Communication ultra distance courte (< 10 cm) , porte-monnaie et carte d'abonnement virtuels
Radio FM	⇒ Radio FM traditionnelle



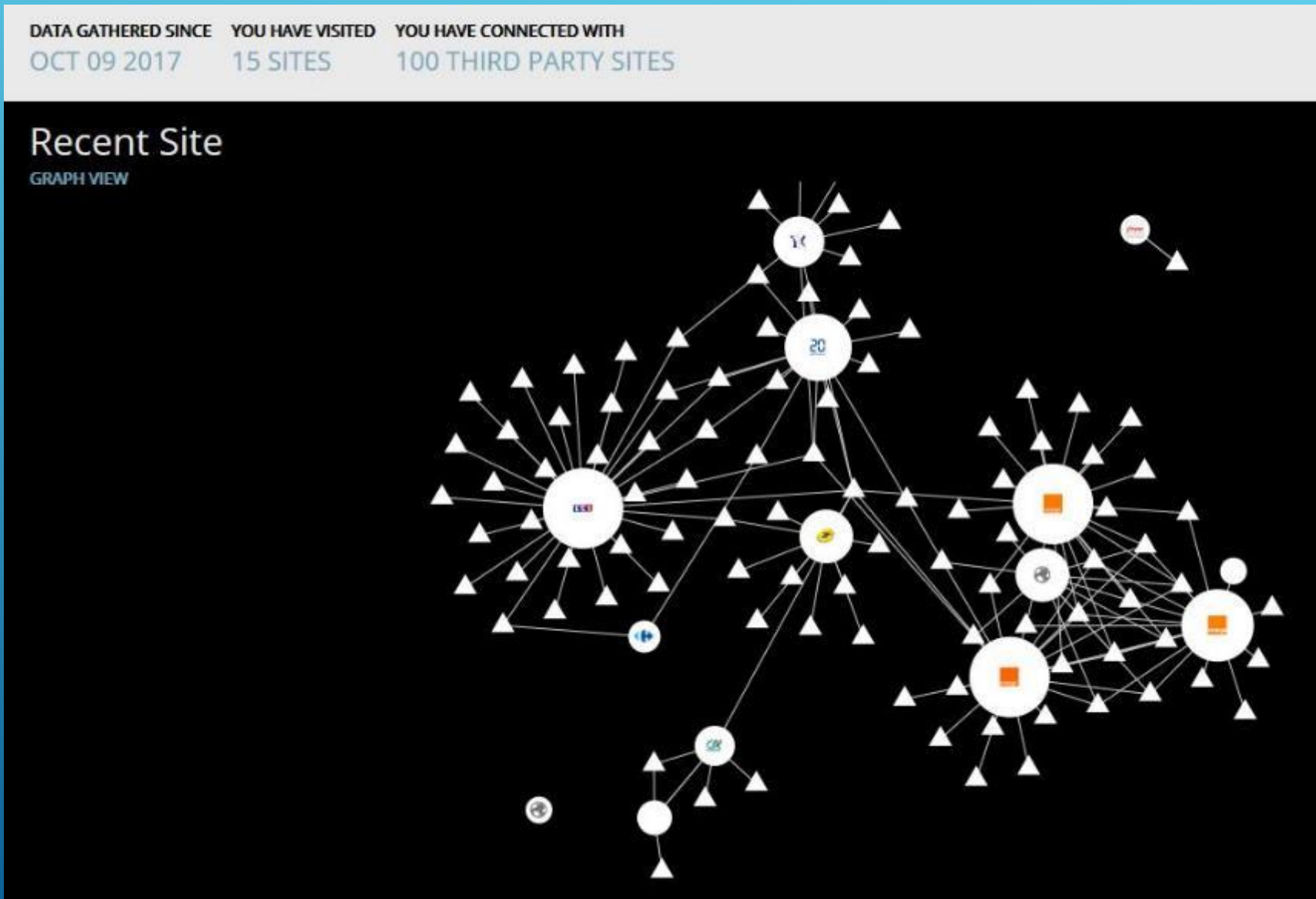
Traçage Wifi



Votre position toujours connue

Même immobile, un smartphone transmet sa géolocalisation 340/jour.

➤ Vous êtes tracés : lightbeam



Archives Google

Qui sont les BATX, ces nouveaux GAFAM asiatiques ?

Google, Apple, Facebook, Amazon, Microsoft - connus sous l'acronyme GAFAM - sont considérés comme les quelques années pourtant, plusieurs groupes asiatiques se posent en sérieux concurrents de ces mastodontes. Leur n

Oubliez les GAFAM, voici venu le temps des BATX, nouveaux géants chinois qui commencent à faire de l'ombre à leurs ri qui vient de dépasser Facebook en bourse, atteignant l'équivalent de 523 milliards de dollars de capitalisation.

Version asiatique des traditionnels Google, Apple, Amazon et de WhatsApp, que font ces nouvelles licornes venus d'Orien

B comme Baidu : Il s'agit du moteur de recherche le plus utilisé en Chine. Comme Google, il propose également aux 6 service de cartographie, des solutions de stockage, de paiement en ligne, et également de la musique et des films.

Créé en 2000, Baidu est devenu le quatrième site le plus visité du monde derrière YouTube, Facebook, et Google. Pour s'in [dû signer un partenariat](#) avec son concurrent iQiyi, filiale du groupe chinois.

Capitalisation boursière : 86 milliards (Bloomberg)

Chiffre d'affaires 2016 : 10,16 milliards de dollars.

A comme Alibaba : Créé en 1999 par Jack Ma, ce businessman incroyable fan de Mickael Jackson, Alibaba ressemble beau lancé 5 ans plus tôt. Toutefois, contrairement au site américain, Alibaba propose également les offres des commerçants loc En 2014, Alibaba entrait dans l'histoire en réussissant alors à Wall Street la plus grande introduction boursière de l'histo dollars. Le groupe revendique 423 millions d'utilisateurs par an.

En moins de quinze ans, le groupe a racheter une bonne partie de ses concurrents e-commerces du pays, et a investi dans d (Youtube chinois) et Sina Weibo (équivalent de Twitter). Un système de paiement a également été créé, permettant de paye restaurants, dans les taxis ou même de payer ses impôts.

Capitalisation : 486 milliards

Chiffre d'affaires 2016 : 15,68 milliards de dollars.

T comme Tencent : Tencent est un groupe spécialisé dans les activités et services sur internet. Messagerie instantanée, site d (façon eBay), réseau social proche de Facebook, jeux en ligne... Le spectre des activités ne cesse de s'élargir.

Créé en 1998, le groupe est connu pour avoir lancé [l'appli à tout faire WeChat](#), qui compte quelques 900 millions d'utilisa

Capitalisation : 520 milliards de dollars

Chiffre d'affaires 2016 : 21,903 de dollars.

X comme Xiaomi : Xiaomi s'est probablement inspiré d'Apple, le design de ses produits est d'ailleurs très proche de celui géant américain, le groupe chinois propose des téléphones portables, mais pas que. Fondé en 2010, soit 34 ans après son pré aussi des téléviseurs, des objets connectés et, même de l'électroménager.

Valorisé à 46 milliards de dollars, Xiaomi, est devenue la troisième plus grosse "licorne" au monde, derrière Uber et son r de CBInsights. Xiaomi ne prévoit d'introduction en bourse avant 2025.

Chiffre d'affaires 2016 : NC.

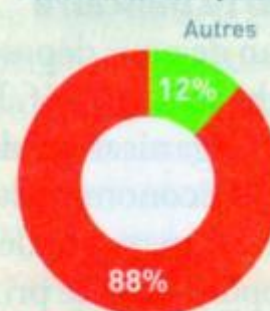
GOOGLE ET FACEBOOK

Rois incontestés de la publicité

Apple et Microsoft gagnent principalement de l'argent avec les produits, les logiciels et les services qu'ils vendent aux consommateurs. En revanche, Facebook et Alphabet (maison mère de Google) vivent quasi exclusivement de la publicité. C'est pourquoi nos données leurs sont précieuses: elles leur permettent de mieux nous connaître et de mieux cibler les annonces.

SOURCES DE REVENUS DES QUATRE GÉANTS DU WEB (2016)

ALPHABET (Google)



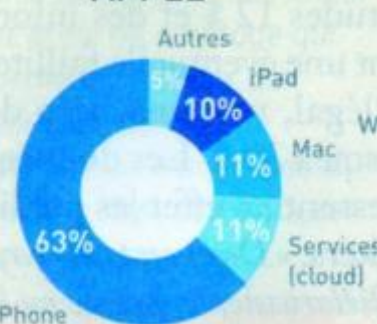
Publicité

FACEBOOK



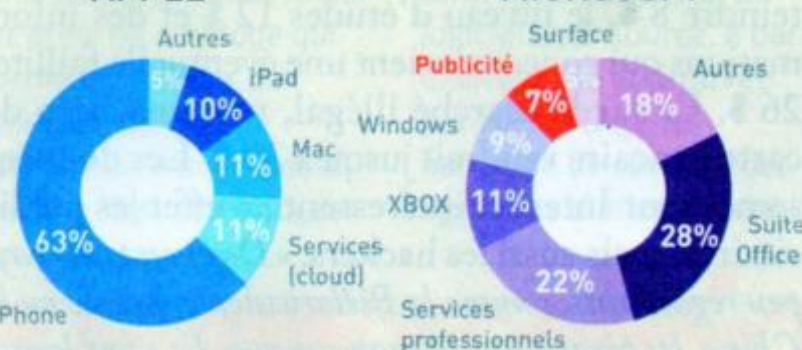
Publicité

APPLE



iPhone

MICROSOFT



Services professionnels

Voici les données recueillies par Google via ces logiciels ou services :

- Les termes que vous recherchez.
- Les vidéos que vous regardez.
- Vos vues de contenu et d'annonces ainsi que vos interactions avec ces derniers.
- Des informations audio et vocales lorsque vous utilisez des fonctionnalités audio.
- L'activité relative aux achats.
- Les personnes avec lesquelles vous communiquez ou partagez du contenu.
- L'activité sur des applications et sites tiers qui utilisent nos services.
- L'historique de navigation Chrome que vous avez **synchronisé avec** votre compte Google.
- Les informations géographiques :
 - Le GPS
 - Adresse IP
 - Les données des capteurs de votre appareil
 - Des informations relatives à des éléments à proximité de votre appareil, tels que des points d'accès Wi-Fi, des antennes-relais et des appareils sur lesquels le Bluetooth est activé

Comment vos données alimentent le ciblage publicitaire

1 VOTRE REQUÊTE

Vous posez une question à votre enceinte (exemple, la météo).



2 RÉPONSE VOCALE

Les serveurs envoient la réponse à l'enceinte : « Il va pleuvoir ».



3 ARCHIVAGE DE VOS DONNÉES

Ces informations, qui reflètent vos centres d'intérêt, sont gardées en mémoire sur d'autres serveurs.



6 LA PUB ARRIVE SUR VOS ÉCRANS

Le ciblage a fonctionné : on vous suggère d'acheter un parapluie.



4 PROFILAGE PUBLICITAIRE

La régie publicitaire analyse ces données et établit des profils de consommateurs. Elle propose ainsi aux annonceurs un public ciblé.



5 COMMERCIALISATION DE VOS DONNÉES

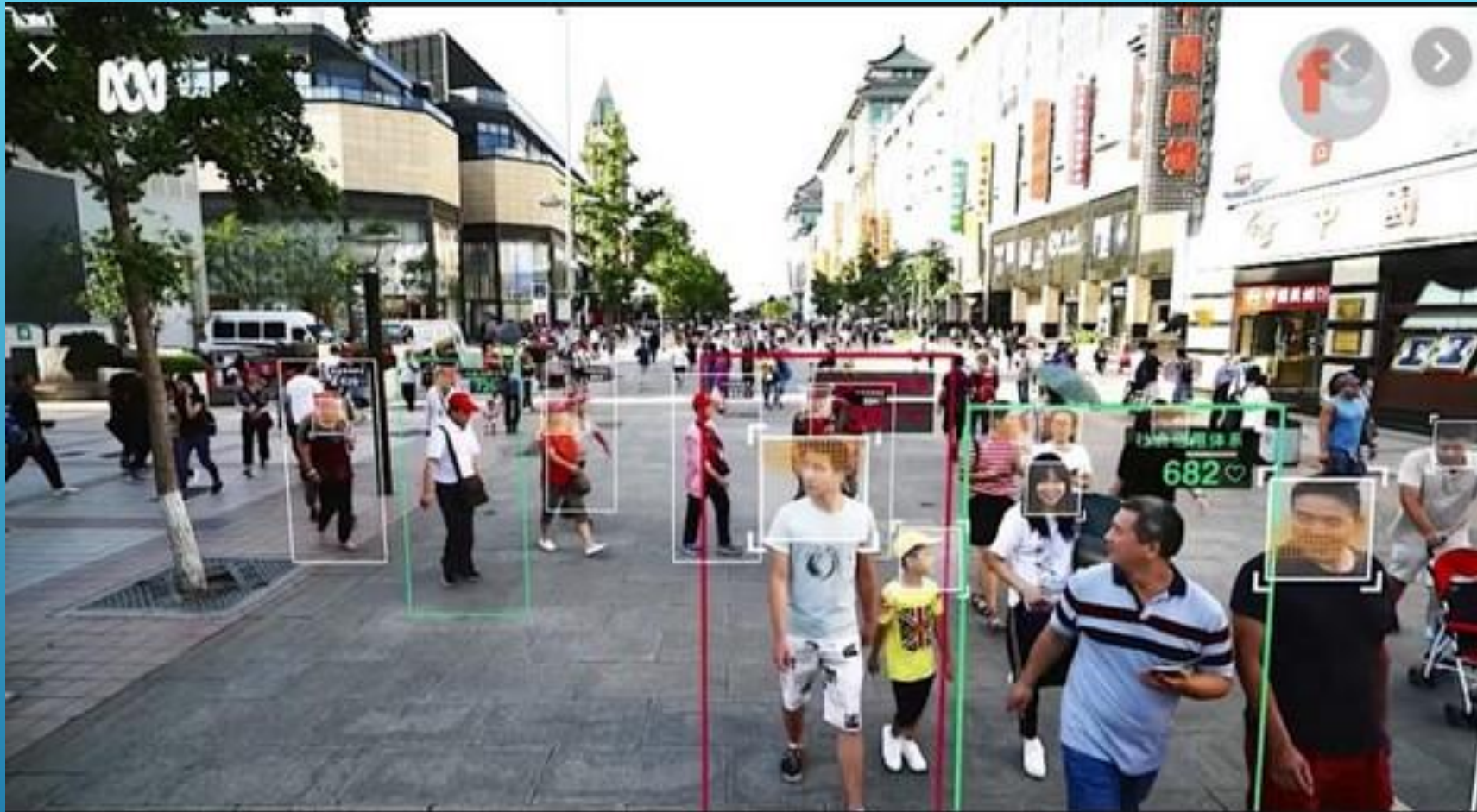
Les annonceurs achètent des emplacements publicitaires, faisant ainsi du marketing personnalisé.



Partage de vos données



Commercialisation de vos données



Le **système de crédit social** est un projet du gouvernement chinois visant à mettre en place d'ici 2020 un système national de réputation des citoyens. Chacun d'entre eux se voit attribuer une note, échelonnée entre 350 et 950 points dite « crédit social », fondée sur les données dont dispose le gouvernement à propos de leur statut économique et social. Le système repose sur un outil de surveillance de masse et utilise les technologies d'analyse du big data. Il est également utilisé pour noter les entreprises opérant sur le marché chinois.

DES SOLUTIONS POUR SE PROTEGER

➤ Naviguez sans être espionné.

➤ Utilisez : FIREFOX  ou BRAVE 

▪ Ajoutez les modules suivants :

- ✓  **Chameleon** une extension complète
Falsifier le profil de
- ✓  **Adblock Plus** bloqueur de publicités
Les publicités, c
- ✓  **Ghostery** détecte les mouchards
Protégez vo
- ✓  **HTTPS Everywhere** active automatiquement
Encrypt the Web! Auto
- ✓  **TrackMeNot** brouiller vos vraies recherches
Protect against
- ✓  **WOT: Web of Trust**,
Par WOT Services Évaluation de la réputation
- ✓  **Malwarebytes Browser Guard**

Chameleon : Falsifier le profil de votre navigateur. Comprends quelques options d'amélioration de la protection de la vie privée.

Adblock Plus : bloqueur de publicités gratuites

Ghostery : Bloqueur de publicité protégeant la vie privée.

HTTPS partout : Chiffrez le Web ! Utilisez automatiquement la sécurité HTTPS avec de

TrackMeNot : Protégez-vous contre le profilage

WOT : vérifie la réputation et les informations de sécurité de n'importe quel site Web en fonction de l'expérience des utilisateurs

Malwarebytes Browser Guard : Il bloque les sites Web malveillants tout en filtrant les publicités gênantes et autres contenus indésirables.

➤ Si vous constatez que vous ne pouvez plus accéder à un site, faites un clic droit sur les icones des extensions pour régler les paramètres. ↗

➤ Utilisez des moteurs de recherche alternatif :

- Startpage 
- Qwant (Français) 
- DuckDuckGo 
- Disconnect Search 
- Seeks 
- Base-search 
- Yippy 

Startpage : est un moteur de recherche qui a pour but de respecter la vie privée.

Qwant : est un moteur de recherche qui a pour but de respecter la vie privée.

DuckDuckGo : est un moteur de recherche qui fait de la protection des données sa

Disconnect Search : permet d'effectuer des recherches anonymes sur Google, Bing, et Yahoo.

Base search : spécialisation universitaire, la capacité de trouver des ressources appartenant au Web profond.

Yippy : est un moteur de recherche qui respecte les utilisateurs et fournit des résultats de recherche équitables basés sur des algorithmes équilibrés.

➤ Utilisez un VPN... (Réseau Privé Virtuel)



 Sweden

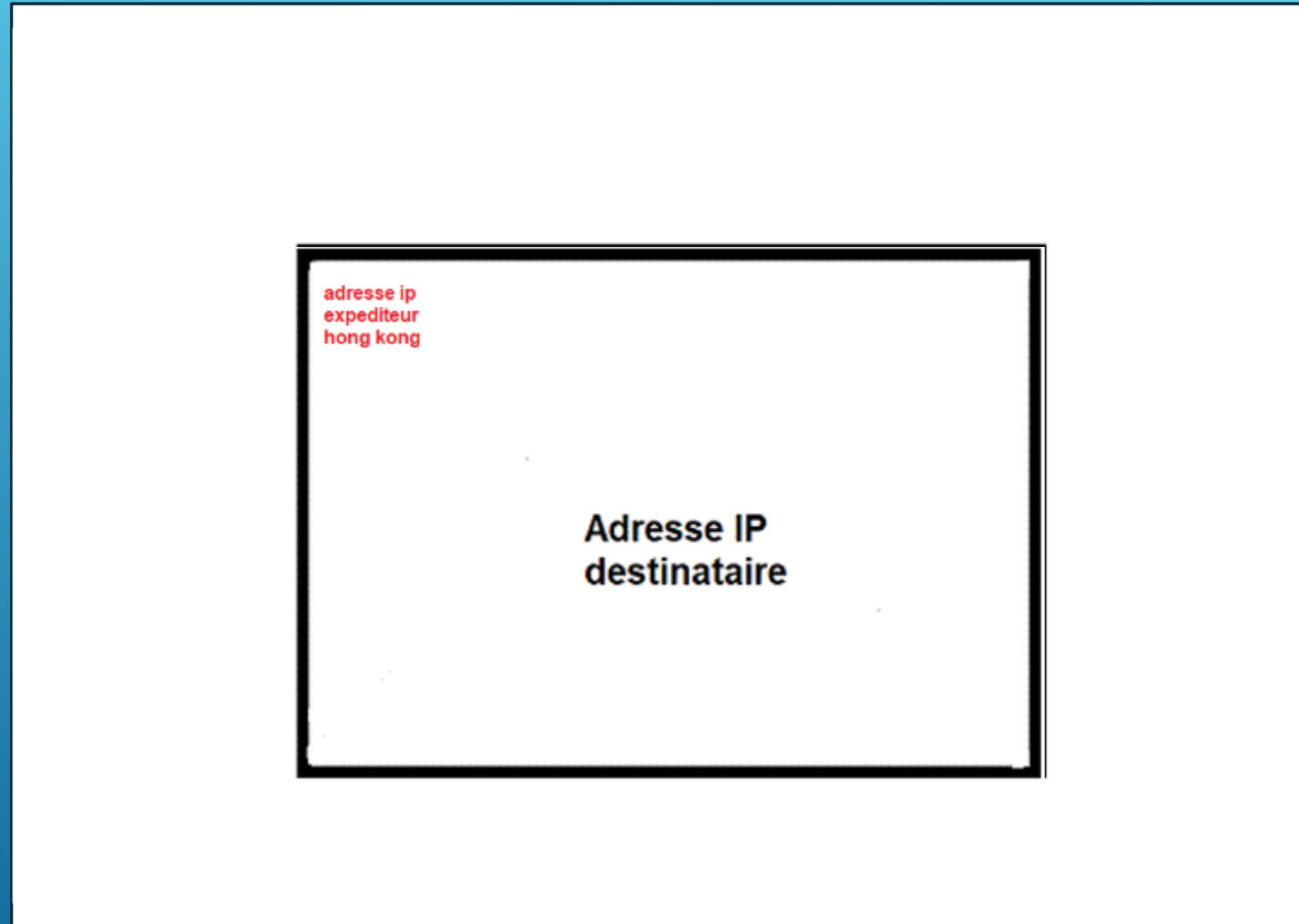
 Turkey

 U.S.A.

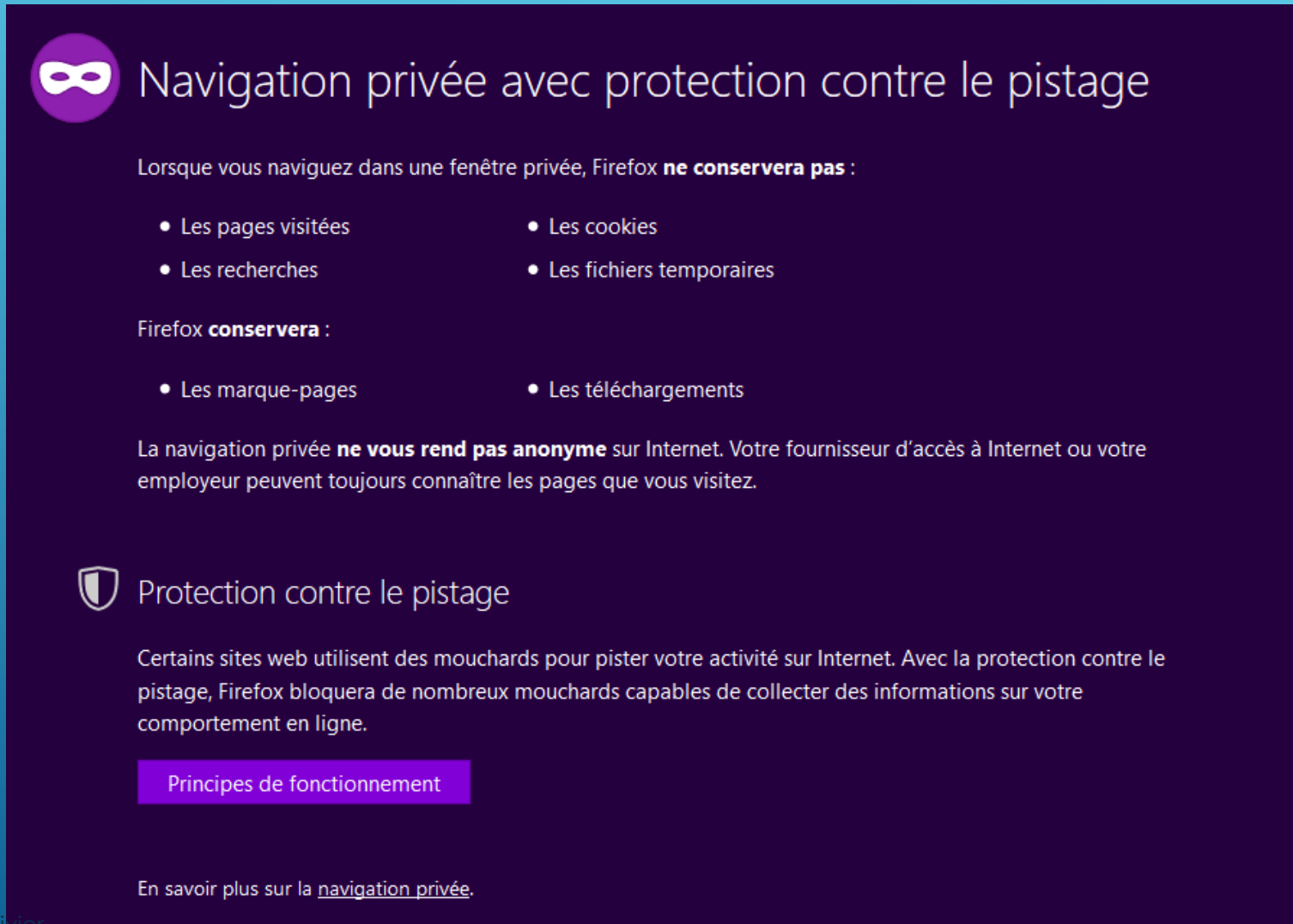
un VPN (*Réseau Privé Virtuel*) comment ça marche?



Guide des VPN



➤ Utilisez la navigation privé :



 **Navigation privée avec protection contre le pistage**


Lorsque vous naviguez dans une fenêtre privée, Firefox **ne conservera pas** :

- Les pages visitées
- Les cookies
- Les recherches
- Les fichiers temporaires

Firefox **conservera** :

- Les marque-pages
- Les téléchargements

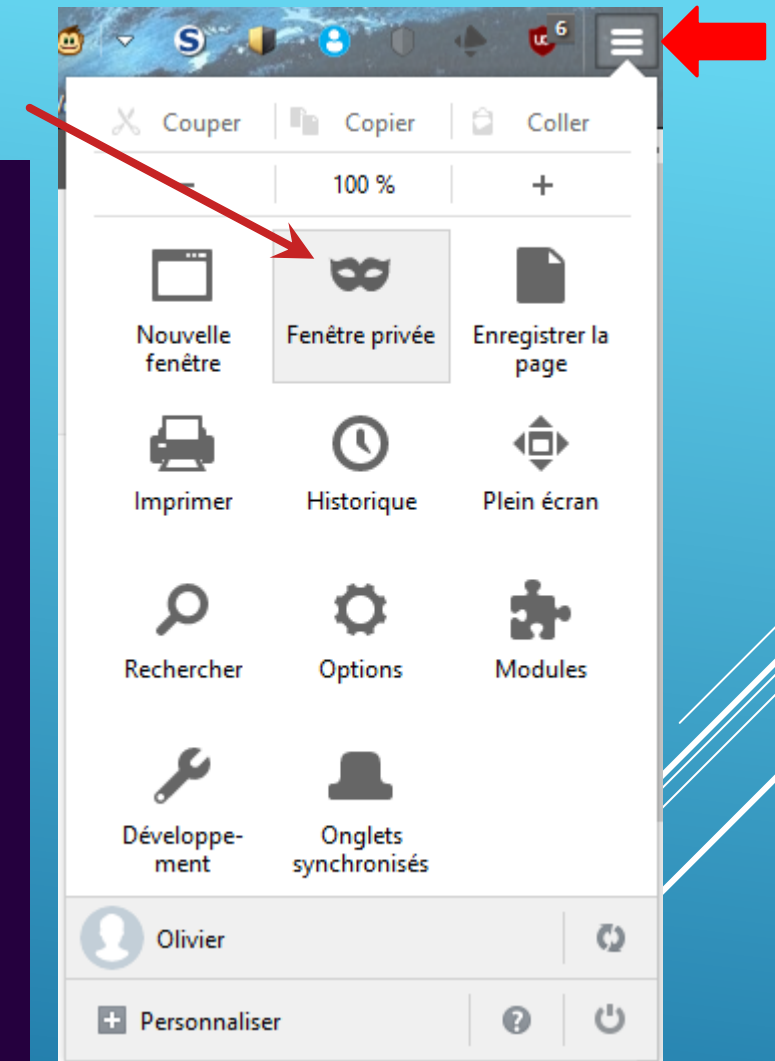
La navigation privée **ne vous rend pas anonyme** sur Internet. Votre fournisseur d'accès à Internet ou votre employeur peuvent toujours connaître les pages que vous visitez.

 **Protection contre le pistage**

Certains sites web utilisent des mouchards pour pister votre activité sur Internet. Avec la protection contre le pistage, Firefox bloquera de nombreux mouchards capables de collecter des informations sur votre comportement en ligne.

[Principes de fonctionnement](#)

En savoir plus sur la [navigation privée](#).



➤ Vous utilisez un WebMail :

The screenshot shows a web browser window with the address bar displaying `https://zimbra.free.fr`. The browser's security information panel is open, showing the following details:

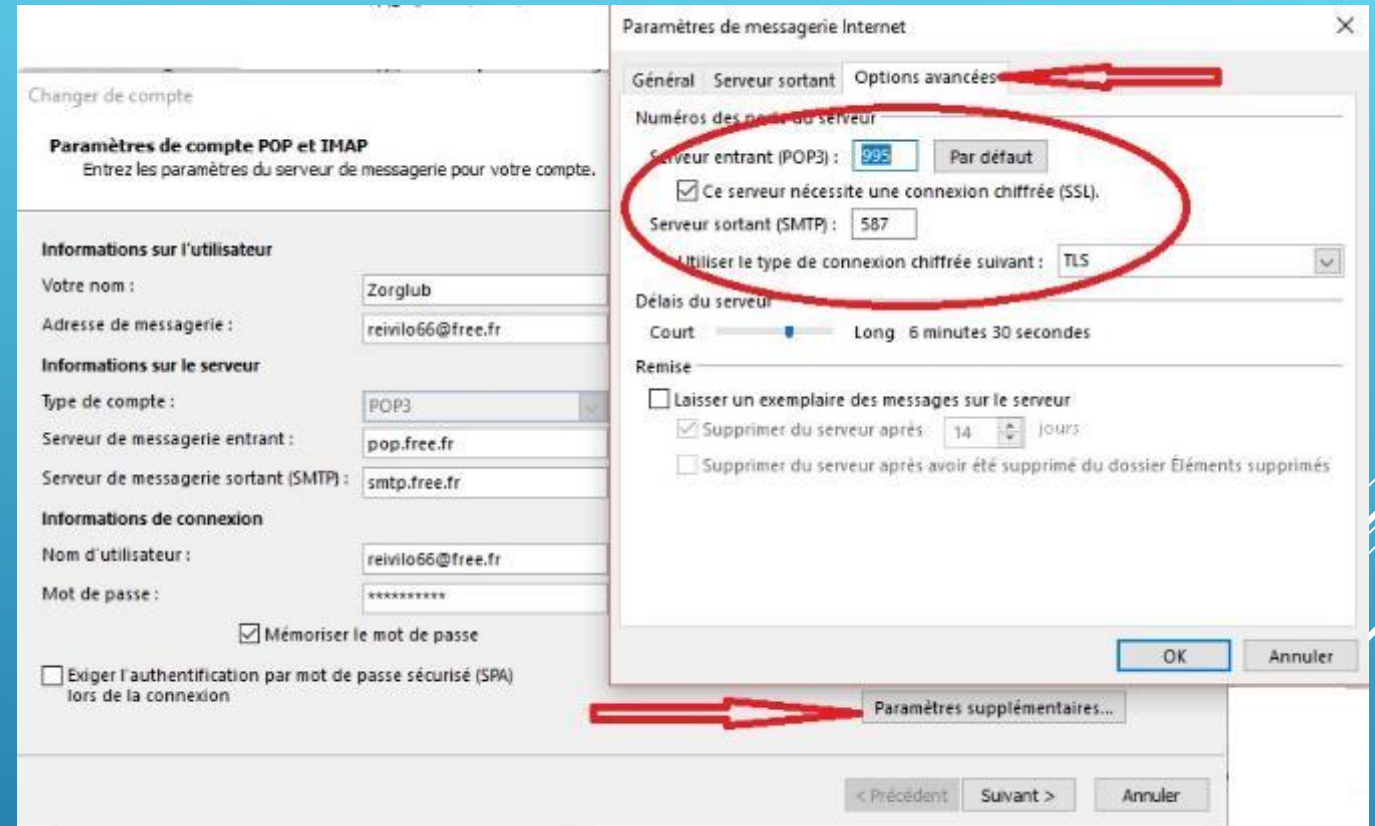
- Identité du site web**
 - Site web : **zimbra.free.fr**
 - Propriétaire : **Ce site web ne fournit pas d'informations sur son propriétaire.**
 - Vérifiée par : **AO Kaspersky Lab**
 - Expire le : **jeudi 7 octobre 2027**
- Vie privée et historique**
 - Ai-je déjà visité ce site web auparavant ? **Oui, 430 fois**
 - Ce site web collecte-t-il des informations (cookies) sur mon ordinateur ? **Oui** (with a [Voir les cookies](#) button)
 - Ai-je un mot de passe enregistré pour ce site web ? **Oui** (with a [Voir les mots de passe enregistrés](#) button)
- Détails techniques**
 - Connexion chiffrée (clés TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bits, TLS 1.2)**
 - La page actuellement affichée a été chiffrée avant d'avoir été envoyée sur Internet.
 - Le chiffrement rend très difficile aux personnes non autorisées la visualisation de la page durant son transit entre ordinateurs. Il est donc très improbable que quelqu'un puisse lire cette page durant son transit sur le réseau.

A red circle highlights the 'Détails techniques' section, specifically the 'Connexion chiffrée' information.

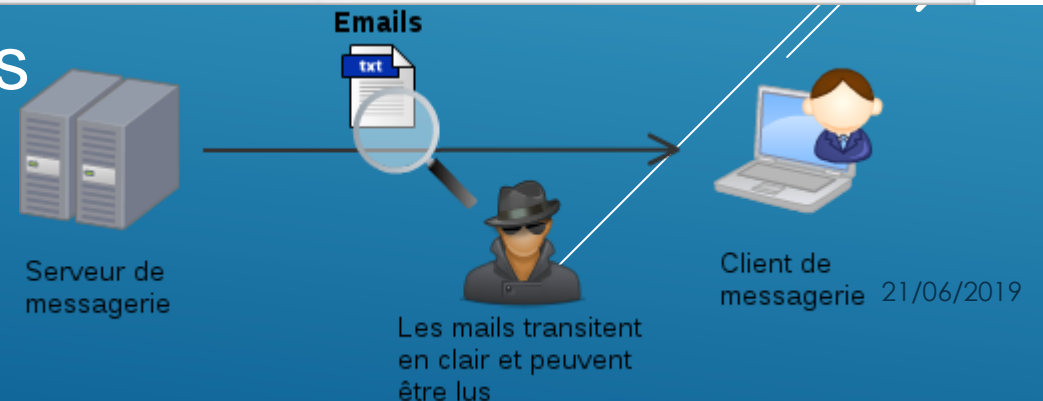
Vérifiez que vous êtes bien en **HTTPS://**

- Vous utilisez un logiciel de messagerie :
Thunderbird, Outlook, IncrediMail, FossaMail, Etc...

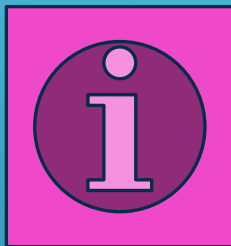
- Vérifiez que vous utilisez bien une connexion chiffrée SSL/TLS



- **Attention** : Si vous utilisez les ports 25 et 110, vos mails transitent en clair et peuvent être lus...



- Principaux numéros de ports, pour utiliser une connexion chiffrée SSL/TLS...



Paramétrer un compte de messagerie

FAI	IMAP / POP / SMTP	N° des ports	chiffrage	SMTP	delais serveur
Orange	imap.orange.fr	993	SSL		
	pop.orange.fr	995	SSL		
	smtp.orange	587	TSL	Authentifier	1
laposte	imap.laposte.net	993	SSL		
	pop.laposte.net	995	SSL		
	smtp.laposte.net	587	TSL	Authentifier	6,5
Gmail	imap.gmail.com	993	SSL		
	pop.gmail.com	995	SSL		
	smtp.gmail.com	587	TSL	Authentifier	6,5
Yahoo	imap.mail.yahoo.fr	993	SSL		
	pop.mail.yahoo.fr	995	SSL		
	smtp.mail.yahoo.fr	587	TSL	Authentifier	6,5
SFR	imap.sfr.fr	993	SSL		
	pop.sfr.fr	995	SSL		
	smtp.sfr.fr	587	TSL	Authentifier	6,5
Free	imap.free.fr	993	SSL		
	pop.free.fr	995	SSL		
	smtp.free.fr	587	TSL	Authentifier	6,5

- Utilisez plusieurs adresses mail

MOTEURS DE RECHERCHE

Au placard, Google!

Google réalise plus de 87% de son chiffre d'affaires grâce à la publicité. Nos données numériques, qui servent au profilage des consommateurs, constituent sa matière première. Lorsque nous cherchons des informations sur son moteur de recherche, nous sommes à la fois fournisseurs (l'historique de recherche en dit long sur nos centres d'intérêt) et clients (les premiers liens qui s'affichent sont des publicités). Certains moteurs de recherche alternatifs assurent qu'ils protègent notre vie privée. C'est le cas de l'américain DuckDuckGo ou du français Qwant. Ce dernier est partenaire de Microsoft Bing pour les

publicités (qui demeurent sa seule source de revenus), mais assure qu'il ne trace pas les internautes. Qwant confesse aussi qu'il complète les résultats de recherche avec ceux de Bing, notamment pour les images (lorsque, sur Google, on limite sa recherche sur « Images », ndlr), en attendant que « tout le Web soit parfaitement indexé ». Le moteur reste malgré tout une alternative intéressante (lire aussi notre enquête sur les moteurs de recherche alternatifs, *QC* n° 557). À titre de comparaison, un internaute rapporte en moyenne 12 € par an à Qwant, et jusqu'à 100 € par an à Google, grâce au ciblage publicitaire!

MESSAGERIE

Créez plusieurs adresses e-mails

Pour ne pas rater un message des impôts ou de la Sécu noyé parmi les publicités et les spams, créez plusieurs adresses e-mails. Un compte pour vos correspondances « sérieuses » (avec les

proches, l'administration, vos contacts du travail, vos loisirs), un autre pour les réseaux sociaux et les forums, et un dernier pour les tiers sans importance (cartes de fidélité, jeux, etc.).

NAVIGATION INTERNET

Halte au pistage

Lorsque vous naviguez sur Internet, vous êtes suivis à la trace. Un petit tour dans les options de votre navigateur (Internet Explorer, Mozilla Firefox, Chrome, Safari) permet de verrouiller quelques paramètres. D'abord, activez l'option « Ne pas me suivre ». Les sites visités seront alertés que vous ne souhaitez pas être pisté (rien ne les contraint à respecter ce choix). Ensuite, bloquez les cookies « tiers », qui ne sont pas indispensables à la bonne navigation. Certains sites demandent au navigateur où vous

êtes. Leur argument est de livrer une information plus précise (les restaurants autour de vous lorsque vous voulez manger une pizza, par exemple). Mais cette donnée est surtout précieuse pour les publicitaires. Dans les paramètres, vous pouvez interdire à votre navigateur de vous géolocaliser. Bloquer les « pop-up » (fenêtres intempêtes) vous épargnera l'affichage de nombreuses publicités. Enfin, lorsque vous utilisez un ordinateur autre que le vôtre, ouvrez une fenêtre de « Navigation privée ». Votre historique

de navigation ne sera pas enregistré, ni vos mots de passe.

COMMENT FAIRE
Accédez aux paramètres de confidentialité et de sécurité de votre navigateur:

► **FIREFOX:** « Outils » puis menus « Vie privée et Sécurité ».

► **INTERNET EXPLORER:** « Réglages » puis « Sécurité » (pour activer « Ne pas me suivre »); « Outils » puis « Options Internet » puis « Confidentialité ».

► **CHROME:** « Réglages » puis « Paramètres » puis « Afficher les paramètres avancés ».

MORT NUMÉRIQUE

Exprimez vos dernières volontés

La loi pour une République numérique d'octobre 2016 instaure le droit de décider du sort de ses données en cas de décès.

Chaque service doit donc permettre aux utilisateurs d'établir un « testament numérique ». Le décret d'application n'est pas encore publié, mais plusieurs plateformes ont pris les devants. Dans les

paramètres de votre compte Facebook, par exemple, il est possible de désigner un contact légataire qui gèrera votre compte après votre décès, ou d'indiquer dès à présent que vous souhaitez que votre compte soit supprimé. Il faudra bien sûr que Facebook ait été prévenu de votre disparition (la

démarche est accessible en ligne). Google a également mis en place un « Gestionnaire de compte inactif » qui permet d'alerter jusqu'à 10 proches ou de supprimer votre compte si vous ne vous êtes pas connecté depuis 3, 6, 9, 12 ou 18 mois.



Les différents WEB'S



Raisons de la non-indexation

- Les sites contiennent de plus en plus de pages dynamiques.
- Certains sites ne sont pas liés par d'autres pages et ne peuvent donc pas être découvertes par les robots d'indexation
- Il faut parfois remplir convenablement un formulaire de critères de recherche pour pouvoir accéder à une page précise.
- Certains sites nécessitent une authentification (requérant un *login* et un mot de passe) avant d'accéder au contenu réel : c'est le cas de certains sites payants et des sites avec des archives payantes (journaux en ligne, bases de données de météorologie, etc.).
- Les pages web peuvent dans leur conception rendre difficile leur indexation. Les balises consistant en un fichier robot.txt inséré dans le code d'une page permettent de protéger son copyright, de limiter les visites ou préserver le site d'accès trop fréquents.
- L'utilisation du langage JavaScript, mal compris par les robots, pour lier les pages entre elles constitue souvent un frein à leur indexation.
- Le web invisible est également constitué des ressources utilisant des formats de données incompréhensibles par les moteurs de recherche.

Web privé

Certaines pages sont inaccessibles aux robots du fait de la volonté de l'administrateur du site web.

Web propriétaire

Le web propriétaire désigne les pages où il est nécessaire de s'identifier pour accéder au contenu.



Des Visa avec leur code pour 35 euros

De nombreux logiciels malveillants sont conçus spécialement pour intercepter les identifiants bancaires et les numéros de cartes de crédit de leurs victimes. Ces données sont ensuite revendues sur Tor. Une carte avec un solde de plus de 2 000 euros, fournie avec son numéro, sa date de validité, son code de vérification et l'identité complète de son propriétaire, sera par exemple vendue 35 euros environ. Les faussaires commercialisent aussi des "skimmers" permettant de récupérer toutes les informations d'une carte bancaire : 1 200 euros pour des dispositifs dotés d'une caméra, d'un faux clavier ou d'un faux lecteur de cartes, qui s'installent sur les distributeurs de billets pour espionner leurs utilisateurs. Enfin, on trouve facilement des identifiants de comptes Paypal. C'est leur solde créditeur qui détermine leur prix. Et charge aux acheteurs de trouver un moyen de retirer l'argent qu'il y a dessus, ou bien de réussir à commander des produits avec, sans pour autant donner leur véritable adresse de livraison...



Dés ordis et iPhone tombés du camion

Les portails de vente les plus fréquentés de Tor, comme Silk Road ou BlackMarket Reloaded, interdisent la vente de produits volés. Mais cela n'empêche pas de nombreux sites de vendeurs indépendants d'en proposer. Le matériel informatique et électronique, avec en vedette les produits Apple et Samsung, est particulièrement bien représenté. On trouve certes de nombreux objets tombés du camion, mais aussi une grande partie de produits "cardés", c'est-à-dire achetés en ligne et payés au moyen de cartes bancaires volées. Contrairement aux produits volés, aisément identifiables par leur numéro de série, les "cardés" sont totalement blanchis. On trouve aussi des cartes cadeaux, utilisables notamment sur le site du e-commerçant Amazon, souvent revendues pour la moitié de leur valeur faciale. Mais le fait qu'on ne puisse pas trouver ces produits volés sur les principales galeries marchandes de Tor augmente le risque d'arnaques car les transactions ne sont pas garanties.



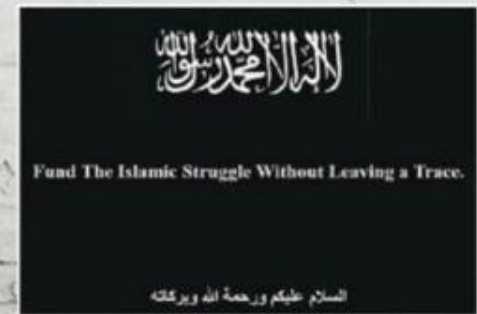
Films de torture et pédopornographie

Toutes les déviances trop étranges ou trop extrêmes pour s'étaler au grand jour sont représentées sur Tor. Y compris le pire du pire, tels les snuff movies, ces films de torture ou de mises à mort bien réelles, et de la pornographie infantile qui se répand également sur des sites payants ou accessibles par cooptation. Certains fonctionnent comme des clubs privés auxquels on n'accède qu'en fournissant soi-même de nouveaux contenus. Néanmoins, selon un habitué du Web interdit, "ceux qui hébergent ou recherchent des contenus pédophiles sont très mal vus sur les réseaux cachés. La plupart des moteurs de recherche et annuaires internes suppriment tout site soupçonné d'héberger de tels contenus". La grande majorité des habitués de ces réseaux dénoncent en effet sans équivoque la pédophilie sous toutes ses formes. Fin 2011, une faction se réclamant d'Anonymous est parvenue à pirater plusieurs sites pédophiles hébergés sur le réseau Tor et à publier des informations personnelles sur leurs utilisateurs.



Militants, dissidents et journalistes

À côté des hors-la-loi, des militants et dissidents politiques se retrouvent aussi sur Tor pour profiter de ses moyens de communications anonymes et chiffrés. Opposants au gouvernement syrien ou extrémistes virulents, les plus actifs ont mis en place des sites de stockage pour partager des documents censurés chez eux : manifestes complotistes ou subversifs, livres interdits, mais aussi manuels pratiques pour déjouer la surveillance de régimes autoritaires... Tor est aussi devenu un point de rendez-vous pour les "whistleblowers", les lanceurs d'alerte. La meilleure illustration en est Edward Snowden, l'ex-employé de la National Security Agency, qui a révélé l'affaire PRISM : il a dénoncé un vaste système de surveillance généralisé orchestré par la NSA et mouillant les plus grands acteurs du Web (Google, Microsoft, Apple, Yahoo...). Vous trouverez une photo de lui avec son PC portable... sur lequel est apposé un autocollant Tor Project.



- Darknet et espionnage économique
- Espace de liberté, anonymat

Espionnage économique de la France : grandes entreprises, chefs d'état, cabinet d'avocats, etc...

La NSA pratiquait aussi l'espionnage économique massif de son "allié" français

Pierre Moscovici et François Baroin, quand ils étaient ministres de

Outils aux services des libertés : il est dangereux de dénoncer les abus des puissants...

Médiapart.

- PME et StartUp qui n'ont pas les moyens de s'offrir un service de protection internet utilisent le Darknet.

Les entreprises françaises scrutées et pillées

L'agence de renseignement américaine avait ciblé "une certaines d'entreprises hexagonales, dont la quasi-totalité de celles cotées au CAC 40", assure Libération. Cet espionnage a pu "aller du simple vol des plans d'étude au pillage de données technologiques confidentielles", mais ce sont surtout "les renseignements sur les appels d'offre impliquant des entreprises américaines" qui intéressait la NSA.

➤ Darknet et libertés (Lanceur d'alertes)

➤ WikiLeaks de l'affaire Julius Bär au Cablegate, reporter sans frontières

➤ **Li Les grandes organisations de journalismes** : journalistes de guerre et journalistes d'investigations, protection des sources et protection des personnes...

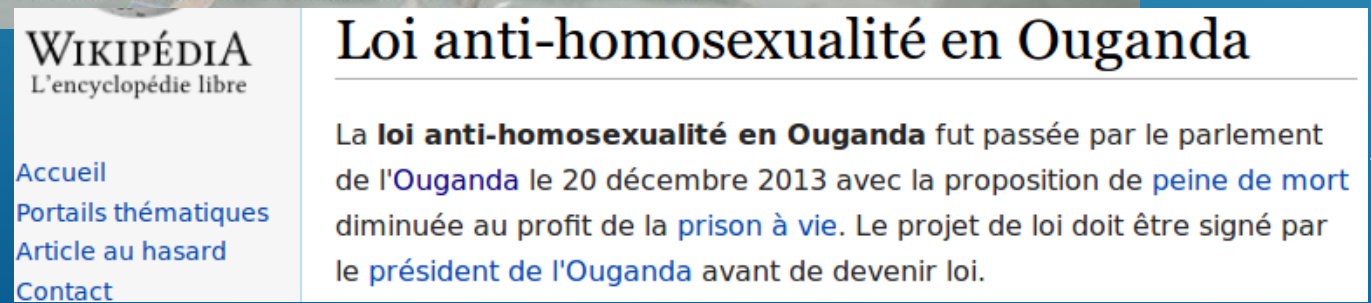
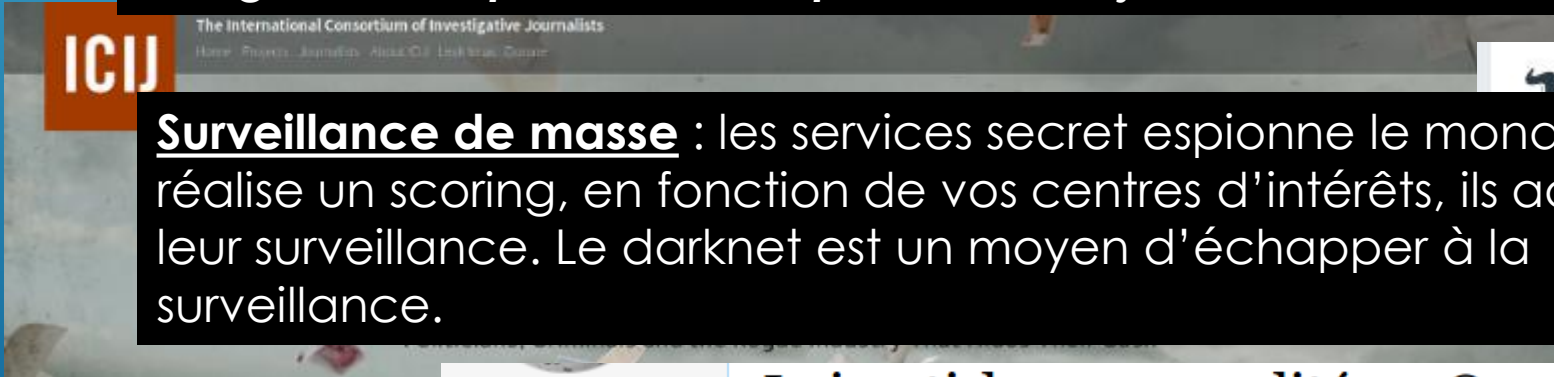
➤ **D** Le NSA a piraté des téléphones Androïde et le BIOS de certains

➤ **La Dissidences** : information du monde sur ce qui se passe dans

➤ **M** -

➤ **Exemple** : Un père qui s'insurgeait que sa fille de 16 ans, recevait des pubs pour des produits de grossesse, Google était au courant avant le père que sa fille était enceinte !!!

▪ **A Google en sait plus sur vous que votre conjoint.**



➤ Les principaux darknets

➤ Tor



Freenet



I2P



- GNUnet,
- Retroshare,
- PGP / GPG,
- Bitmessage,
- Signal, Wire, Skred.
- Telegram, Chat Secure, Alrawi, etc.
- Et des dizaines d'autres (PrivaTegrity, etc.).

Doc : <https://www.youtube.com/watch?v=V8cnzyJ7S4s&feature=youtu.be>

Vous avez des questions?



Comment se protéger



C I E L

CLUB INFORMATIQUE EDUCATIF LAURENTIN

www.ciel-laurentin.fr

06 68 33 92 96