Big Brother is watching you : quelle vie privée à l'heure des réseaux sociaux et du Cloud ?

Estelle Debouy conférence du

10 mars 2020

Plan de la conférence

Liens utiles

— Le tracking en ligne : https://donottrack-doc.com/fr/episode/2

— Vérifier l'authenticité d'une information sur internet : http://www.hoaxbuster.com/ et https://www.lemonde.fr/les-decodeurs/

— Privacy Badger : https://www.eff.org/fr/privacybadger.

— Empêchez Facebook de vous suivre partout sur Internet : https://addons.mozilla.org/fr/firefox/addon/facebook-container/
— Pour le partage de fichiers en toute confidentialité : https://upload.disroot. org/.
— La CNIL : https://www.cnil.fr/fr/maitriser-mes-donnees
— « Des millions de comptes Yahoo ! piratés en 2014 », FR3, 23 sep 2016 : http://sites.ina.fr/cnil-40-ans/focus/chapitre/5/medias/5823342_001_014
— L'extension Web Of Trust de Firefox : https://addons.mozilla.org/fr-FR/firefox/ addon/wot-safe-browsing-tool/
— Comment réagiriez-vous si votre boulanger exigeait l'accès aux mêmes informations que vos applications ?: https://www.nouvelobs.com/rue89/rue89-internet-actu/20150210.RUE7727/et-si-notre-boulanger-exigeait-l-acces-aux-memes-infos-que-nos-app html
— Outil de chiffrement facile à utiliser : AxCrypt (https://www.axcrypt.net/fr/).
— Chiffrer ses mails : https://www.mailvelope.com/
— La Free Software Foundation : http://www.fsf.org/
— Module complémentaire de protection de la vie privée dans Firefox : http://ftp.gnu.org/gnu/gnuzilla/ (choisir ensuite votre version de Firefox, et cliquer sur privacy_ext.xpi)
— Prism break : http://prism-break.org/fr
— Module *Adblock Plus* pour bloquer la publicité : https://addons.mozilla.org/fr/ firefox/addon/adblock-plus/
— Un bon moteur de recherche : https://www.startpage.com/fr/search/privacy-policy.html ou encore https://duckduckgo.com/
— Un logiciel de gestion de vos mots de passe : https://keepass.info/

Textes cités

1 Internet et le paradoxe de la vie privée

Propos de Bill Thompson lors de la conférence Lift en 2009 à Berlin :

Les utilisateurs de Twitter et autres outils de réseaux sociaux, partagent plus de données, avec plus de gens que le FBI de Hoover ou la Stasi n'auraient jamais pu en rêver. Et nous le faisons de notre propre chef, espérant pouvoir en bénéficier de toutes sortes de manières.

2 Traces à tous les étages

Définition des données personnelles d'après les articles 2 et 8 de la Loi informatique et libertés de 1978 :

Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. [...]

Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales, ethniques, les opinions politiques, philosophiques, religieuses ou l'appartenance syndicale, ou qui sont relatives à la santé ou à la vie sexuelle des personnes.

3 Le darknet

Suétone écrit dans la *Vie de César*, 56 5 :

On possède enfin de César des lettres à Cicéron, et sa correspondance avec ses amis sur ses affaires domestiques. Il y employait, pour les choses tout à fait secrètes, une espèce de chiffre qui en rendait le sens inintelligible (les lettres étant disposées de manière à ne pouvoir jamais former un mot), et qui consistait, je le dis pour ceux qui voudront les déchiffrer, à changer le rang des lettres dans l'alphabet, en écrivant la quatrième pour la première, c'est-à-dire le D pour l'A, et ainsi de suite [1].

À vous de jouer : **DOHD MDFWD HVW**

E. Snowden : « répondre "je n'ai rien à cacher" en matière de vie privée revient à affirmer qu'on se fiche de la liberté d'expression parce qu'on n'a rien à dire ». G. Greenwald, *Nulle part où se cacher*, Lattès, 2014 :

Prises dans leur intégralité, les archives Snowden conduisent à une conclusion fort simple : le gouvernement américain a bâti un système qui s'est fixé comme objectif l'élimination complète, à l'échelle planétaire, de toute vie privée électronique.

Gilles Deleuze, « Post-scriptum sur les sociétés de contrôle », *Pourparlers*, 1990 :

Nous entrons dans des sociétés de contrôle qui fonctionnent, non plus par enfermement, mais par contrôle continu et communication instantanée. [...] Face aux formes prochaines de contrôle incessant en milieu ouvert, il se peut que les plus durs enfermements nous apparaissent appartenir à un passé délicieux et bienveillant. [...] L'important ce sera peut-être de créer des vacuoles de non-communication, des interrupteurs, pour échapper au contrôle.

Wikileaks déclare sur son site [2] :

Les principes généraux sur lesquels notre travail s'appuie sont la protection de la liberté d'expression et de sa diffusion par les médias, l'amélioration de notre histoire commune et le droit de chaque personne de créer l'histoire. Nous tirons ces principes de la Déclaration universelle des droits de l'homme. En particulier l'article 19 inspire le travail de nos journalistes et autres volontaires.

[1] . De façon insolite, le code de César a été réemployé notamment au début d'internet et des forums, à travers le ROT-13. Le ROT-13 désigne simplement le code de César, où on a choisi une ROTation de 13 lettres (A–>N...). L'idée n'est pas de diffuser des messages cryptés, mais de faire en sorte que le message ne soit pas lu involontairement, par exemple s'il dévoile l'intrigue d'un film ou donne la réponse à une devinette.

2. Voici le texte original : « The broader principles on which our work is based are the defence of freedom of speech and media publishing, the improvement of our common historical record and the support of the rights of all people to create new history. We derive these principles from the Universal Declaration of Human Rights. In particular, Article 19 inspires the work of our journalists and other volunteers. » (source : https://wikileaks.org/About.html).

4 Comment se protéger : les quatre conseils faciles à suivre

Un bon mot de passe ? Exemple : **Rns2cifpà.**

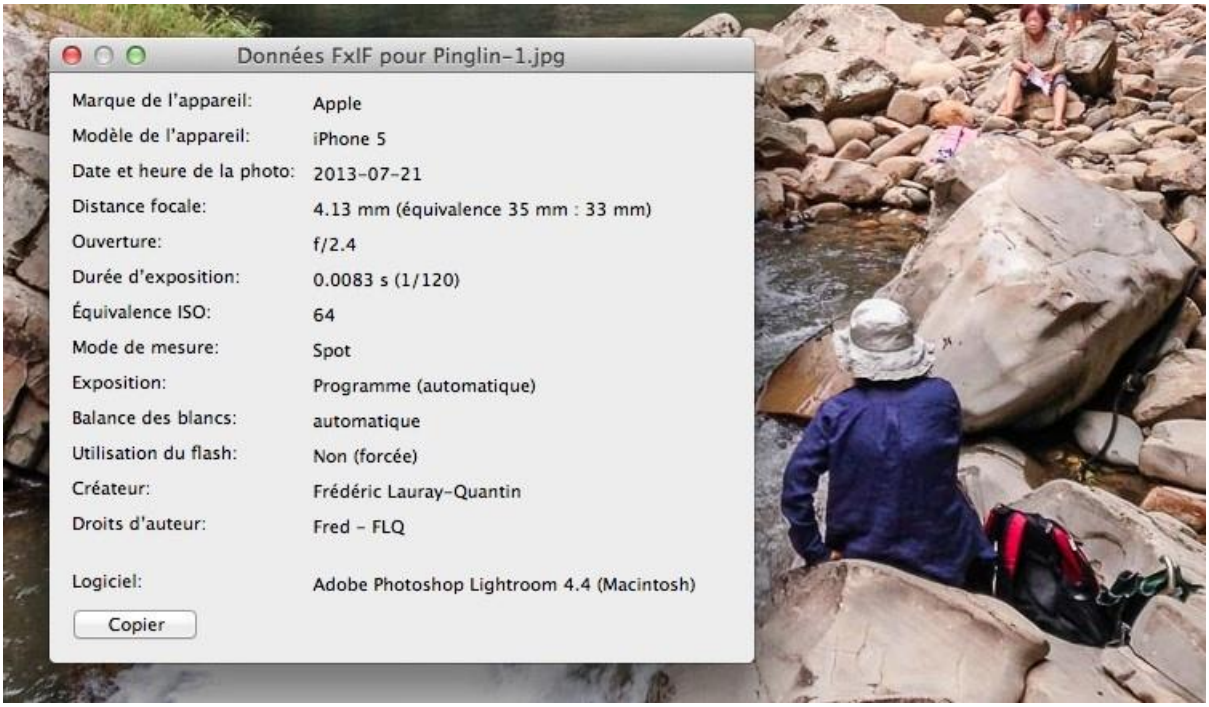

Figure 1 – Exemple de métadonnées dans un fichier image

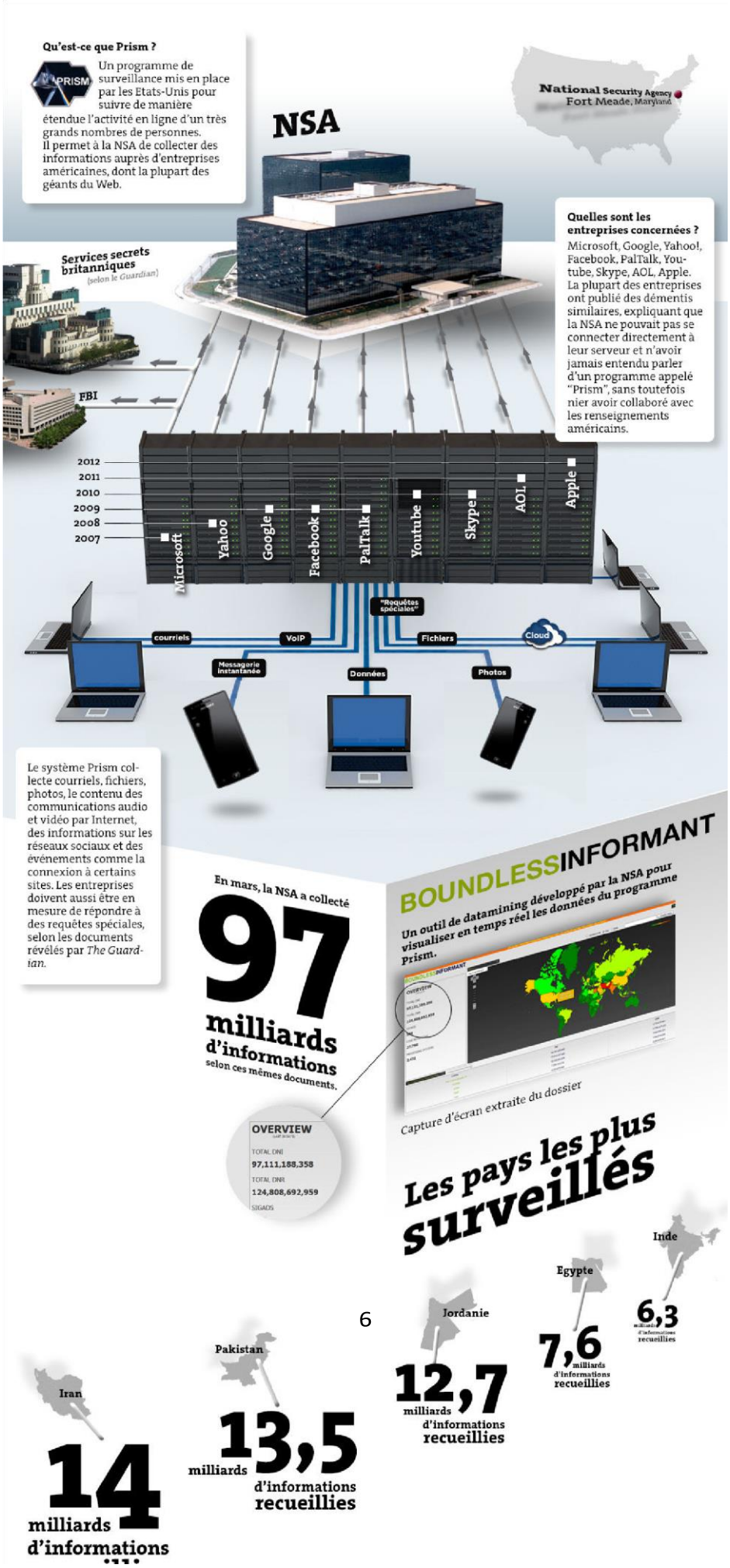
Qu'est-ce que Prism ?
PRISM
Un programme de surveillance mis en place par les Etats-Unis pour suivre de manière étendue l'activité en ligne d'un très grands nombres de personnes.
Il permet à la NSA de collecter des informations auprès d'entreprises américaines, dont la plupart des géants du Web.
NSA
National Security Agency
Fort Meade, Maryland
Quelles sont les entreprises concernées ?
Microsoft, Google, Yahoo!, Facebook, PalTalk, Youtube, Skype, AOL, Apple. La plupart des entreprises ont publié des démentis similaires, expliquant que la NSA ne pouvait pas se connecter directement à leur serveur et n'avoir jamais entendu parler d'un programme appelé "Prism", sans toutefois nier avoir collaboré avec les renseignements américains.
Services secrets britanniques
(selon le Guardian)
FBI
2012
2011
2010
2009
2008
2007
Microsoft
Yahoo
Google
Facebook
PalTalk
Youtube
Skype
AOL
Apple
"Requêtes spéciales"
courriels
VoIP
Fichiers
Cloud
Messagerie instantanée
Données
Photos
Le système Prism collecte courriels, fichiers, photos, le contenu des communications audio et vidéo par Internet, des informations sur les réseaux sociaux et des événements comme la connexion à certains sites. Les entreprises doivent aussi être en mesure de répondre à des requêtes spéciales, selon les documents révélés par The Guardian.
En mars, la NSA a collecté
97
milliards
d'informations
selon ces mêmes documents.
OVERVIEW
TOTAL DNI
97,111,188,358
TOTAL DNR
124,808,692,959
SIGADS
BOUNDLESSINFORMANT
Un outil de datamining développé par la NSA pour visualiser en temps réel les données du programme Prism.
Capture d'écran extraite du dossier
Les pays les plus surveillés
Inde
6,3
milliards d'informations recueillies
Egypte
7,6
milliards d'informations recueillies
Jordanie
12,7
milliards d'informations recueillies
Pakistan
13,5
milliards d'informations recueillies
Iran
14
milliards d'informations

Figure 2 – Vie privée de Firefox

• • • LE MONDE — 21 mars 1974 — Page 9

JUSTICE

Tandis que le ministère de l'intérieur développe la centralisation de ses renseignements

Une division de l'informatique est créée à la chancellerie

En ordre dispersé, les départements ministériels tentent de développer à leur profit, à leur seul usage, l'informatique et son outil, l'ordinateur. Ce n'est pas tout à fait un hasard si, à l'époque où le Journal officiel va publier un arrêté créant une « division de l'informatique » au ministère de la justice, celui de l'intérieur met la dernière main à la mise en route d'un ordinateur puissant destiné à rassembler la masse énorme des renseignements grapillés sur tout le territoire; pas un hasard non plus si le projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus) destiné à définir chaque Français par un « identifiant », qui ne définisse que lui, maintenant terminé, est l'objet de convoitises ardentes; le ministère de l'intérieur y souhaite jouer le premier rôle. En effet, une telle banque de données, soubassement opérationnel de toute autre collecte de renseignements, donnera à qui la possédera, une puissance sans égale.

Ainsi se trouve d'évidence posé un problème fondamental, même s'il est rebattu : celui des rapports des libertés publiques et de l'informatique. Son importance exigerait qu'il en fût, au Parlement, publiquement débattu. Tel ne paraît pas être, pourtant, la solution envisagée par le premier ministre dans les directives qu'il vient d'adresser au ministère de la justice, intéressé au premier chef si l'on s'en rapporte à la Constitution qui dans son article 66 fait de l'autorité judiciaire le gardien des libertés individuelles.

« Safari » ou la chasse aux Français

Rue Jules-Breton, à Paris-13e, dans des locaux du ministre de l'intérieur, un ordinateur Iris-80 avec bi-processeur est en cours de mise en marche. A travers la France, les différents services de police détiennent, selon la confidence faite par un très haut magistrat, 100 millions de fiches, réparties dans 400 fichiers. Ainsi se trouve posées — et, à terme, théoriquement résolues — les données d'un problème comprenant, d'une part, l'énormité des renseignements collectés ; de l'autre, la méthode à définir pour faire de cet ensemble une source unique, à tous égards, de renseignements.

L'histoire du très puissant appareil qu'est l'Iris-80 est exemplaire du secret qui entoure l'épanouissement de l'informatique dans les administrations, quelles que puissent être les informations qui filtrent ici et là.

l'origine, budgétairement, n'était pas du tout prévu pour la tâche qu'il a finalement assurée, mais pour « traiter » les données administratives du Fichier national des constructeurs (F.N.C.). Il s'agit donc apparemment d'un détournement manifeste de crédits d'études, ce qui n'était sans doute pas le vœu du Parlement qui les vota.

De vastes ambitions

Il n'y a pas que cela. Le ministère de l'intérieur a d'encore plus vastes ambitions. Détenteurs, déjà, du fichier national du remembrement, les services de M. Jacques Chirac font de grands efforts pour, affirme-t-on, s'en adjoindre d'autres : le cadastre, le fichier de la direction nationale des impôts et, plus grave peut-être, celui du ministère du

Ce n'est pas, pourtant, que les avertissements aient manqué. Le Conseil d'Etat en 1970, puis le ministère de la justice en 1970 (qui avait rappelé le rôle dévolu à l'autorité judiciaire de « *gardien des libertés individuelles* » et donc réclamé voix au chapitre) ont insisté sur la nécessité d'une intervention législative qui préciserait les quelques éléments essentiels de l'emploi de l'informatique appliquée aux particuliers : réglementation de l'acces des tiers aux fichiers, de l'intercommunication de ceux-ci, droit de rectification des personnes fichées si les renseignements retenus sont inexacts, etc.

De plus, tous les exemples étrangers incitent à ce débat sur une utilisation de l'informatique à laquelle, par définition, il ne s'agit pas de renoncer, mais à qui doivent être tracées des limites, si grand

outil, il n'apparaît pas — sauf erreurs négligeables, relativement — que l'accès des tiers ou le droit à contrôle des personnes visées — par demande d'un extrait — ait jamais provoqué des bavures préjudiciables à la légalité.

De même, le fichier national des conducteurs, dans sa partie judiciaire, est prévu par une loi, et il faut regretter que les textes d'application ait permis des illégalités injustifiables — mais connues (*le Monde* du 8 mars).

« A la hussarde »

Fort, pourtant, de ces avantages, le ministère de la justice paraît curieusement se laisser dépasser par des querelles internes peu compréhensibles. L'arrêté signé le 18 mars par M. Jean Taittinger le montre.

dite commission. D'autant qu'il est d'ores et déjà connu que M. Touffait a été rayé de la liste des « sachants ». Il semble d'ailleurs que les réactions vives qui sont enregistrées portent moins sur le renouvellement des structures, jugées inévitables, que sur la méthode « *à la hussarde* » employée par tel membre de l'entourage de M. Taittinger pour mener à bien ses projets de rénovation de la gestion dans le domaine judiciaire.

Est-ce à dire de plus que les choix que l'on entend promouvoir soient nécessairement les plus opportuns ? Tout indique, pour l'instant, que, si le ministère de l'intérieur a définitivement choisi le « matériel lourd » pour s'équiper, la chancellerie, au contraire, s'oriente vers un réseau de mini-ordinateurs placés auprès de chaque tribunal de grande instance important.

d'un *aggiornamento* technique, a illustré son discours par un large reportage sur les équipements du tribunal de Bobigny — plus réduits, donc plus rapides à réaliser, ainsi plus vite source d'orgueil pour leurs créateurs.

C'est donc un doute global qui pèse sur les intentions du gouvernement, en général, et du ministère de la justice, en particulier : ce dernier département, qui rappelle à tous sa mission de protection des libertés individuelles, a apparemment accepté sans broncher la suppression d'un éventuel débat public, ce qui jette sur les déclarations « libérales » de M. Taittinger en d'autres domaines une suspicion qui n'est pas de bon aloi.

Mais, dans cette entreprise, le ministère de la justice, même s'il fait preuve d'une grande maîtrise pour

Figure 3 – Article du *Monde* du 21 mars 1974

Figure 4 – Enigma 1940 (Wikimedia Commons, licence CC BY-SA 3.0)

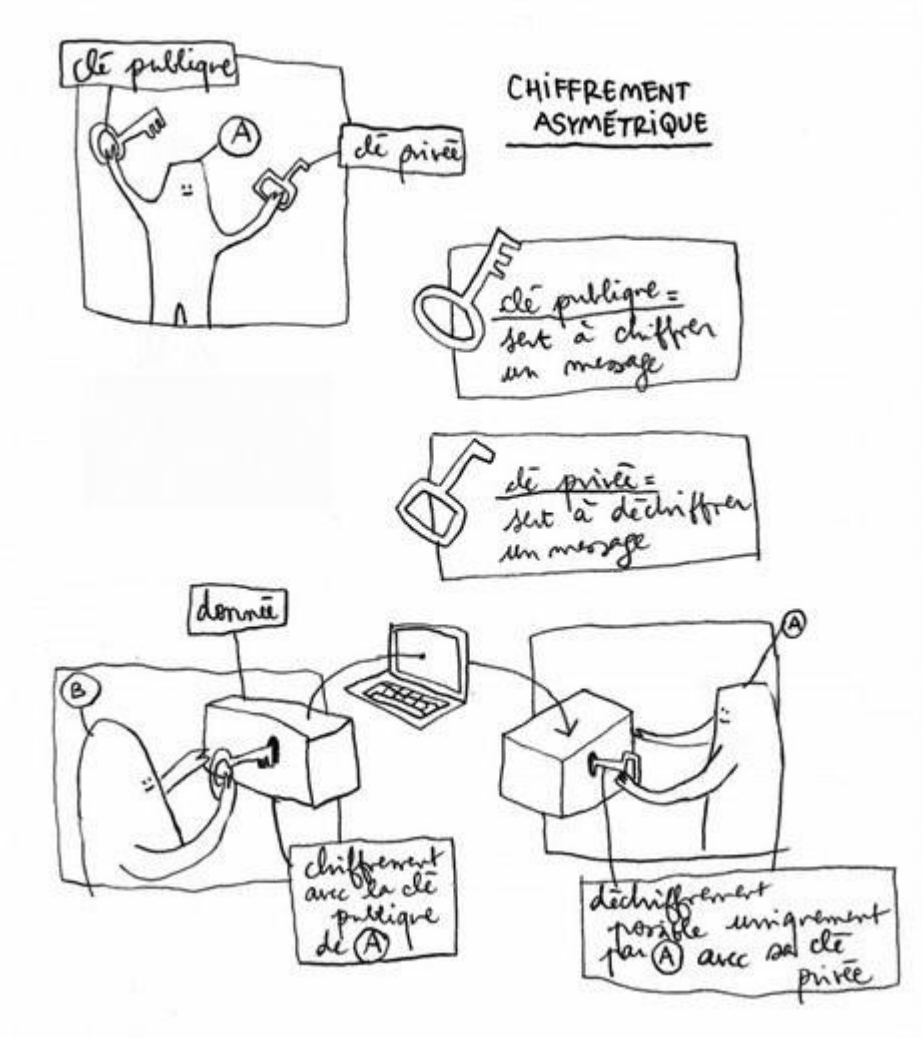

Figure 5 – Chiffrement asymétrique

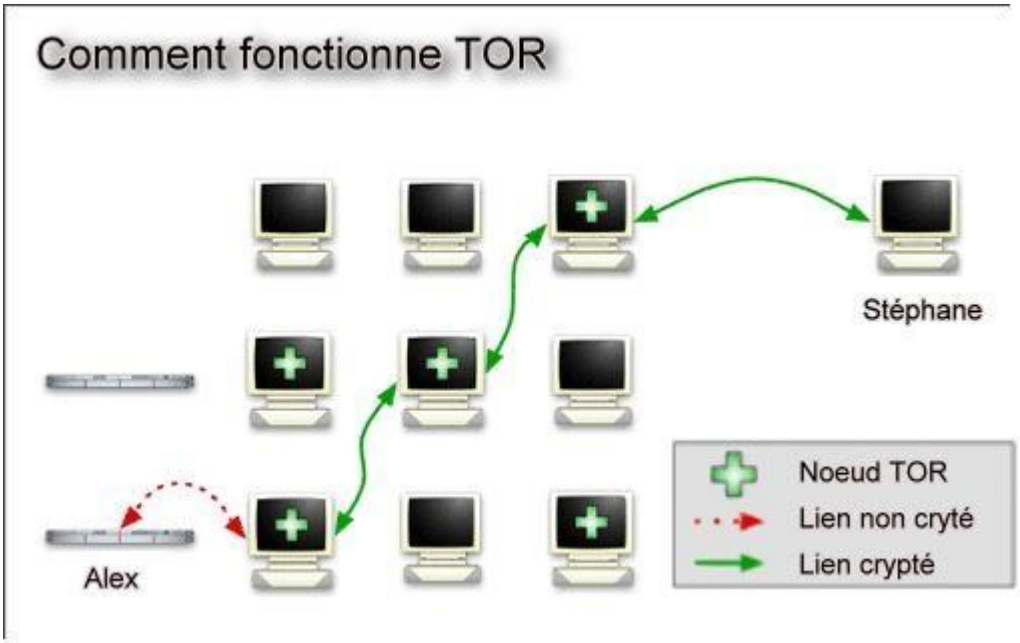

Figure 6 – Comment fonctionne Tor

Figure 7 – Soumettre des documents à Wikileaks