# Reset the Net

## Une initiative citoyenne de protection de la vie privée

**9e Journées de l'informatique IN2P3-IRFU**
13-16 octobre 2014

**Claude Zurbach**

**LUPM**

# Sommaire

- **Internet : un réseau en constante mutation dans sa technique et son usage**
- **Anonymat et vie privée à l'ère de la surveillance électronique de masse**
- **Lanceurs d'alertes : leurs motivations et leur impact**
- **La protection des données au niveau individuel : la panacée ?**
- **Reset the Net, un exemple d'initiative issue de la société civile**
- **Connaissance et responsabilité ?**

# Internet : un réseau en mutation

## Risque de saturation ?... Incidences du passage en V2...

Quelques faits marquants :

Une explosion des données individuelles avec l'apparition de l'Internet V2, "collaboratif"et disposant d'accès individuels rapides (plus d'un milliard de comptes Facebook aujourd'hui, 700 millions de smartphones connectés, 600 millions de blogs...)

Des enjeux économiques déterminants aussi du point de vue fonctionnel que prospectif

Des enjeux dits "sécuritaires" se renforçant proportionnellement au volume de données

De profondes évolutions induites dans les processus cognitifs, voir dans le simple rapport au réel

L'apparition constante de nouvelles applications liés à la masse de données, entraînant des évolutions sociales et économiques

Un développement et une amélioration constante de méthodes et outils d'extraction de connaissance, sur tous les types de médias et supports

Un réseau qui tend à se transformer en champ de bataille où les enjeux sont politiques, économiques et militaires.

Et malgré cela, un réseau dont les techniques au sens “hardware” sont basées sur des évolutions majeures remontant à 20, 30, voir 40 ans... et dont les infrastructures souffrent aujourd'hui du manque d'investissements publics.

Une connaissance qui se perd : la complexité et l'aspect composite du réseau des réseaux est parvenue à un point où la maîtrise même de l'outil va s'avérer difficile, ou réservée à une élite pas forcément toujours bien intentionnée.

# Anonymat et vie privée

## Anonymat, protection et créativité

L'anonymat (qui peut se traduire sur le réseau en *pseudonymat*) permet la communication,

la collaboration avec l'assurance que votre véritable identité est protégée aussi longtemps que vous en décidez ainsi. La volonté de s'exposer n'est donc pas incompatible avec celle de se protéger.

Le choix de l'anonymat permet la créativité et donne un espace de liberté.

De fait, l'anonymat est inscrit dans la loi en ce qui concerne le droit de vote, et personne n'imaginerait imposer une traçabilité sur vos choix électoraux …

Pourtant, la **traçabilité** - l'ennemi de l'anonymat - reste volontairement mal contrôlée le droit reste ici à construire, malgré quelques décisions de justice allant dans le bon sens aux Etats-Unis ou en Allemagne (deux exemples parmi d'autres).

## Vie privée

Ce concept n'est pas figé : il est variable selon les règles qui régissent la place de l'individu dans les sociétés humaines. Néanmoins dans notre société, c'est un droit fondamental.

"Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance" (*article 8, Convention européenne des droits de l'homme*)

Article 12 de la Déclaration universelle des droits de l'homme, articles 226-1 à 226-7 du Code pénal, article 9 du Code civil, Loi Informatique et Libertés de 1978...

Nous avons théoriquement le droit en France d'exiger d'un service la destruction des données nous concernant.

La réalité aujourd'hui : des **données** qui sont **tracées**, **saisies**, **traitées**, **redistribuées** sans que nous soyons à même de les effacer, voir d'en être simplement informés.

## Anonymat et vie privée

### "Je n'ai rien à cacher, alors où est le problème ?"

Argument fréquemment invoqué, et facilement démontable.

Nous avons toujours quelque chose à conserver à l'abri de n'importe quel regard : un numéro de carte bancaire, un problème de santé, des conversations privées, des situations où l'on était pas à son avantage #;-) voir des infractions même mineures.

Ce qui est autorisé ou non est à géométrie variable, évolue avec le temps et les contextes sociaux, économiques et politiques. L'exemple de l'aide aux personnes en situation dite irrégulière en est un exemple frappant.

C'est aussi prendre le problème à l'envers... C'est justement intolérable d'être surveillé parce que justement nous n'avons rien à nous reprocher !

Et d'un point de vue plus philosophique : les attitudes induites par le sentiment d'une surveillance possible, réelle ou supposée, mènent à la soumission et au conformisme le plus plat, toutes choses qui empêchent une société d'évoluer.

En résumé : plus rien ne garantit aujourd'hui que vos données personnelles ne parviennent pas en de mauvaises mains, soient mal exploitées dans des contextes de forte concurrence (par exemple pour une embauche) ou que dans 10 ans les règles sociales n'aient pas changé. Autant de raisons de renforcer l'utilisation de l'anonymat sur Internet.


Dad says you're spying us online
He's not your dad

## Lanceurs d'alertes : leurs motivations et leur impact

### Le facteur humain

Mais la machine finit se par gripper... Un dispositif aussi complexe et faisant intervenir autant d'individus doit forcément connaître des failles.

Internet étant un peu le lieu du "tout et n"importe quoi" en termes de publication, il ne suffit pas de mettre en ligne des documents classés confidentiels et impliquant des institutions étatiques ou autres pour que le réseau fasse caisse de résonance. Un grand nombre de barrages existent.

Il est possible de classer les "lanceurs d'alerte" en deux catégories :

- le phénomène Wikileaks, avec ceux qui diffusent des documents dévoilant au grand jour des comportements hautement condamnables (exemple de Bradley Manning qui décida de rendre publiques certaines des atrocités commises par l'armée américaine en Irak),
- ceux qui comme Edward Snowden veulent dénoncer avant tout des méthodes totalement illégales de surveillance électronique de masse, plus que divulguer un contenu ciblant un contexte ou une affaire en particulier.

Pour cela il importe de procéder avec méthode, en connaissant les rouages de la presse et en sachant anticiper le comportement “du réseau”.

Les motivations d'Edward Snowden sont explicitées dans l'ouvrage de Glenn Greenwald "No Place to Hide" (titre français : "Nulle part où se cacher" paru aux éditions J.C Lattès)

# Lanceurs d'alertes : leurs motivations et leur impact

## Des révélations qui créent le choc

Les révélations d'Edward Snowden, rendues publiques à partir du 6 juin 2013, commencent avec un important volume de documents (d'abord estimé entre 15 et 20 000, chiffre ensuite constamment réévalué à la hausse pour atteindre 1,7 million en décembre 2013).

Ces documents sont transmis par Edward Snowden à deux journalistes, Glenn Greenwald et Laura Poitras, et progressivement à travers plusieurs titres de presse.

Ils concernent la **surveillance mondiale d'internet**, mais aussi des **téléphones portables** et autres moyens de communications comme les lignes intercontinentales où transitent l'essentiel des communications mondiales... principalement par la **National Security Agency américaine** (NSA).

Ils dénoncent une étroite collaboration entre la NSA et les principales entreprises du Web (Google, Yahoo, YouTube, Skype...) par l'intermédiaire du programme **Prism** ou US-984XN.

## ... Et la France n'est pas en reste

"*Le Monde est en mesure de révéler que la Direction générale de la sécurité extérieure (DGSE, les services spéciaux) collecte systématiquement les signaux électromagnétiques émis par les ordinateurs ou les téléphones en France, tout comme les flux entre les Français et l'étranger : la totalité de nos communications sont espionnées.*
*L'ensemble des mails, des SMS, des relevés d'appels téléphoniques, des accès à Facebook, Twitter, sont ensuite stockés pendant des années.* " Révélations sur le Big Brother français – 4 juillet 2013

De plus, tout un arsenal législatif a été voté ces dernières années pour tenter d'étendre et légaliser les pratiques des services français du renseignement.

# Comment la France intercepte les communications

## 1 La captation

Communications téléphoniques, e-mails, SMS, fax... L'expéditeur et le receveur sont identifiés ; la durée, la fréquence et la localisation sont enregistrées.

**Satellites espions**

**Données électromagnétiques interceptées**

**Câbles sous-marins (fibre optique)**
Transport des communications Internet et téléphoniques

**Stations d'écoute**
Une vingtaine de stations réparties sur le territoire métropolitain et les DOM-TOM


## 2 Le stockage

**Direction générale de la sécurité extérieure (DGSE)**
Boulevard Mortier à Paris
Un des plus puissants supercalculateurs de France, il est installé sur trois étages en sous-sol.

## 3 L'accès aux données

- **DGSE** Direction générale de la sécurité extérieure
- **DCRI** Direction centrale du renseignement intérieur
- **DNRED** Direction nationale du renseignement et des enquêtes douanières
- **DPSD** Direction de la protection et de la sécurité de la défense
- **DRM** Direction du renseignement militaire
- **Tracfin** Traitement du renseignement et action contre les circuits financiers clandestins
- **Service du renseignement de la Préfecture de police de Paris**

### La DGSE en chiffres

**600** millions d'euros de budget et **40** millions d'euros de fonds spéciaux

**4 991** personnes dont 28 % de militaires

**687** embauches de 2009 à 2014, essentiellement des ingénieurs

INFOGRAPHIE *LE MONDE* PHOTO AFP

## Gérer au mieux soi-même la confidentialité des données

Sans attendre de solutions collectives et à grande échelle, il est possible de traiter à son niveau le problème de la protection des données en faisant le choix au cas par cas d'exploiter une solution de cryptage s'appuyant par exemple sur des algorithmes à clefs asymétriques.

"*Le principe des algorithmes cryptographiques à clefs asymétrique repose sur deux clefs. L'une privée (Ks), qui sera l'information secrète. L'autre publique (Kp), que l'on distribue à tout le monde. L'algorithme de cryptage est f(m,K)=m' avec K une clef, m un message et m' le message crypté.*" Linux-France.org

Autant parler d'une **solution éprouvée : PGP** ou **Pretty Good Privacy -** puisqu'il s'agit de celle adoptée par Edward Snowden lui-même pour sécuriser ses communications avec les journalistes Glenn Greenwald et Laura Poitras.

## PGP et GPG

**PGP** est un logiciel de cryptage remontant à 1991 et développé par Phil R. Zimmerman puis très largement distribué sur le réseau. La loi américaine interdisant l'exportation de logiciels cryptographiques, cela lui valut une enquête criminelle gouvernementale de trois ans. PGP est aujourd'hui distribué par Symantec™, en version payante.

Ce logiciel est basé sur un cryptage à base de clefs asymétriques de type RSA, algorithme mis au point en 1977 et dont le brevet (MIT) a expiré en septembre 2000.

**GnuPG** ou **GNU Privacy Guard** est une implémentation complète et libre de droits de PGP. GnuPG est une application référencée RFC2440 (OpenPGP), et il est compatible avec PGP. Il faut noter que le projet a été soutenu dès 2000 par le gouvernement fédéral allemand.

Pour exemple, **Ubuntu** livre de base une version **gnupg2**, avec différents interfaces graphiques de gestion (attention : 2 correctifs pour les versions 10.04. 12.04) et différents *plugins*.

## Reset the Net


### Un exemple d'initiative plus collective et issue de la "société civile"

**http://resetthenet.tumblr.com**

"*Nous avons la technologie nécessaire, et l'adoption du cryptage est la première étape efficace que tout le monde peut prendre pour mettre fin à la surveillance de masse. C'est pourquoi je suis très heureux de l'initiative* ***Reset the Net*** *- qui marquera le moment où nous transformons l'expression politique en actions concrètes, et où nous nous protégeons sur une grande échelle. [...] Joignez-vous à nous le 5 juin, et ne sollicitez pas pour votre vie privée. Prenez-la en main*" – Edward Snowsden

Bien qu'il soit difficile de mesurer l'ampleur réelle de ce mouvement, plusieurs centaines d'organisations et d'associations (essentiellement du monde anglo-saxon) s'y sont associées, en s'engageant à utiliser et à promouvoir :

### The Privacy Pack

Le **Reset the Net privacy pack** est une sélection de logiciels et de conseils adaptés pour les ordinateurs classiques, les téléphones et les tablettes que quiconque peut utiliser.

L'objectif est d'offrir ces solutions à tous, ainsi que des outils en bonus et des instructions pour les utilisateurs plus avertis. Une fois ces outils généralisés, il devrait être facile pour tout un chacun de partager avec les interlocuteurs de son choix les données de la vie privée.

Les **outils recommandés** pour iPhone, Android, Mac, Windows et GNU/Linux, et le tout sous forme de logiciels libres:
Adium et Pidgin pour communications sur Gtalk, Facebook, Yahoo, MSN, XMPP/Duck Duck Go et d'autres, - TextSecure et RedPhone pour Android et iPhone, pour les SMS et les appels vocaux privés - HTTPS Everywhere pour les navigateurs - GPGtools et Enigmail en *bonus* pour les utilisateurs plus techniques) – Tor (Onion Routing Project) en bonus pour les utilisateurs plus avancés ou ceux ayant des besoins d'anonymat.

# Conclusion : réinvestir ses connaissances sur la Toile ?


## Une capacité à comprendre et donc à maîtriser l'Internet qui risque de s'affaiblir

La complexité atteinte par le réseau aujourd'hui (protocoles de communication de plus en plus composites, multiplication des recommandations et standards, hétérogénéité des systèmes raccordés et des applications déployées...) rend de plus en plus difficile la maîtrise de tout le dispositif.

Les ingénieurs et techniciens disposant de cette connaissance ne devraient-ils pas tous réinvestir et partager leurs connaissances sur la Toile au profit de tous les utilisateurs ?

## L'anonymat absolu n'existe pas

Nous sommes bien placés pour savoir qu'il n'est pas d'anonymat absolu sur le réseau, et que d'une façon ou d'une autre tout est "traçable".

Mais les barrages que nous pouvons mettre en place pour protéger la confidentialité des données devraient rendre impossible une surveillance de masse qui nécessiterait alors des ressources de calcul inimaginables...

## Comment choisir ses armes ?

Les outils de protection mis en place doivent être communs au maximum d'utilisateurs (se fondre dans la masse), basés sur des solutions libres ou *open source* (garantie de qualité, sans but lucratif).