« Tout le monde espionne tout le monde »[1]

- Rappel de faits

¶ Il y a quelques mois, Edward Snowden, ancien employé de l'agence de Sécurité Nationale Américaine, la NSA, révélait les activités de surveillance —ou d'espionnage— top secrètes de cette institution gouvernementale au service du FBI et de la CIA. Ce que révèle Snowden, c'est que la NSA écoute et enregistre les métadonnées d'un nombre inimaginable de conversations téléphoniques et d'activités internet de citoyens lambda, partout sur le globe[2], sois couvert de lutte contre le terrorisme. Pour cela, la NSA utilise le programme Prism[3], qui relève d'un accord avec les plus grandes entreprises web à ce jour, telles que Google, Facebook, APple etc. et lui permet d'utiliser les informations récoltées de leurs internautes stockées sur leurs serveurs. La NSA peut également croiser et tracker toutes les informations en ligne—recherches, mails, crenseignements, goûts, photographies etc.—sur la personne qu'elle veut surveiller grâce au programme XKeyScore[4]. Enfin, la NSA puise en temps réel dans les flux de données, directement via les infrastructures réseau (tour relais de télécommunication, câble sous-marins et fibre optique) grâce à un programme d'écoute et de « traque » nommé Upstream[5]. Ces pratiques sont aussitôt dénoncées par la Commission Nationale de l'Informatique et des Libertés (CNIL)[6], dont la mission est de « protéger la vie privée et les libertés dans le monde numérique » et une plainte est portée en justice par l'Electronic Frontier Foundation (EFF) et dix-sept autres associations américaines[7]. Cela relance le débat de la gestion des données numériques générées par l'internaute.

¶ Le fait est qu'aujourd'hui, ces données sont générées de manière quasi-constante par notre utilisation d'outils à technologie numérique, et la récupération et le stockage de ces informations intéressent bon nombre de marques, de publicitaires, d'institutions et bien sûr les gouvernements ! Ainsi la traque de ces renseignements sur les citoyens semble se systématiser : nos téléphones portables, nos ordinateurs, nos GPS etc. peuvent en dire long sur le quotidien et l'identité de chaque citoyen à travers les données ou data qu'ils génèrent. La récupération et l'utilisation de ces data recouvre en réalité un véritable enjeu aujoud'hui et pour l'avenir, car ces données offrent un fort potentiel économique aux intéressés. En attendant, la question alimente la polémique de « l'espionnage » des citoyens et intenautes et du non respect des libertés fondamentales : on retient le scandale des poubelles hi-tech Londoniennes qui se sont avérées, après un an, être en réalité capable de reconnaître chaque smartphone se présentant à proximité et ainsi révéler à l'insue de leur propriétaire leur habitudes de vie en terme de géo-localisation et de consommation[8]. Ces data ont donc potentiellement le pouvoir de dire où je suis et où j'étais, quand, avec qui, ce que j'ai acheté, l'endroit où je me suis attardé et pendant combien de temps... Une somme d'informations qui intéresse forcément les entreprises et institutions gouvernementales.

¶ De manière générale on est assez mal à l'aise avec cette notion de surveillance ; pourtant on peut se demander si la collecte et la surveillance de ces data ne dérangent pas surtout ceux qui ont quelque chose à se reprocher. Après tout, si moi, citoyen lambda, je n'ai rien à me reprocher ; en quoi le fait que mes données Facebook -par exemple- soient surveillées par la NSA me dérangent dans mon utilisation quotidienne d'internet ?

• On peut penser en effet que ces datas scrutées par les instances de renseignements dérangent surtout les citoyens qui ne sont pas en accord avec la loi.

¶ Il faut savoir que cette activité d'écoute et de stockage de métadonnées réalisée de manière très large sur l'ensemble des citoyens de la planète par la NSA, s'est instaurée après les attaques terroristes du 11 septembre 2001. Il ne s'agit sûrement pas d'une cause en soi, mais plutôt d'une juxtaposition de circonstances qui ont laissés penser aux autorités américaines que tous les moyens étaient bons pour lutter contre le terrorisme. Il convient de noter qu'après les attaques, les enquêtes menées pas les agences de renseignements américaines auprès des agences de renseignements européennes, ont montrés que des indices révélaient la planification de cet attentat notamment dans les données concernant les allers-retours de plusieurs protagonistes entre l'Allemagne et l'Iraq[1]. En théorie, une surveillance accrue et la révélation de ces données auraient pu empêcher le drame du 11 septembre 2001. Dès lors, on peut réellement se demander si cette activité de surveillance de chaque citoyen n'est pas une manière de chercher à protéger une population contre les individus qui

voudrait la mettre en danger. Pour moi, citoyen lambda en accord avec la loi, ce serait donc un apport pour améliorer ma sécurité.

¶ Par ailleurs, le cas de data récoltées par la NSA n'est qu'un exemple. Aujourd'hui, la plupart de nos objets technologiques génèrent ces data[1]. A chaque passage sur internet, les navigateurs comme Chrome par exemple, sont capables de renseigner les recherches que vous avez effectuées, de connaître les mots-clés de vos mails, les pages que vous consultez régulièrement etc. Votre fournisseur internet est lui capable de renseigner vos horaires de connexions, les adresses web sur lesquelles vous surfez. C'est en partie sur ces datas que s'appuient les services de police dédiés à la lutte contre la cyber-criminalité. Dans ce cas, ces datas peuvent donc permettre la protection des citoyens face aux actes illégaux de quelques individus. Autre exemple : nos GPS. Ils sont eux capables de renseigner à chaque instant la vitesse à laquelle nous roulons, vers où nous nous déplaçons, à quels endroits nous nous arrêtons. Ils permettent de suivre la trace d'une personne en infraction avec la loi qui chercherait à fuir ou même en théorie renseigner sur les individus ne respectant pas les limites de vitesse et conduisant dangereusement.

¶Enfin, l'utilisation de ces data peut même potentiellement rendre des services plus personnels. La plupart du temps, c'est même ce qui fait l'argument des géants qui enregistrent vos datas : en échange, ils vous proposent un service. C'est le cas de Facebook, de Google, d'Apple et bien d'autres. En échange d'un service proposé, quel qu'il soit, ces géants se servent des datas que nous générons pour faire du profit. Facebook par exemple, stocke chaque donnée de chacun de ses utilisateurs sur ses serveurs. Cela lui sert d'avantage auprès des annonceurs pour mieux cibler les messages publicitaires, pour mesurer l'impact de ces derniers ou encore pour utiliser les « like » comme argument de vente : si votre ami aime cette marque, vous serez d'avantage susceptible de l'aimer et de la liker pour lui faire savoir. C'est ainsi que les marque deviennent populaire sur Facebook et gagnent en visibilité. C'est ce qu'on appelle « publicité sociale ». Google lui, utilise la création des données de navigations et des cookies pour passer des accords commerciaux[9] au niveau du référencement des sites web sponsorisés. De manière concrète, il propose de faire apparaître tel ou tel site promotionnel en haut des résultats de recherche selon le profil de l'utilisateur. Enfin, pour les navigateurs, cela leur permet de vendre des espaces publicitaires ciblés : par exemple, après avoir visité un site de voyage, des annonceurs de séjours touristiques vous proposent un encart publicitaire pour un voyage similaire sur chaque page qui suivra. Toute la question est de savoir si ces pratiques sont acceptables ou non. Dans le cas de Facebook ou Google, les data collectées servent aussi à améliorer le service et les moteurs de recherches. Si un utilisateur continu d'utiliser ces services web, c'est évidemment qu'ils y trouvent un intérêt. L'échange « data contre service optimisé et personnalisé » peut alors être considéré comme légitime. Dans le cas des profits réalisés via les annonceurs publicitaires, le fait est que ces encarts de publicité existeront quelque soit la page : il est peut-être préférable alors que la publicité proposée soit en lien avec mes intérêts et mes anciennes recherches, plutôt qu'elle n'est aucun rapport avec moi...

¶Ces dernières pratiques sont directement issues de l'héritage marketing qui dans la publicité a toujours cherché à référencer ses clients potentiels, devenant des « cibles », dont il faut connaître les goûts et intérêts pour adapter le discours et donc l'argument de vente. Quant aux pratiques de suveillance ou d'espionnage il faut noter que dans les domaines industriel ou politique il s'agit d'une pratique ancienne, comme les écoutes gouvernementales et policières par ailleurs largement reconnues comme faisant partie des politiques de sécurité nationale[1]. Seuls les moyens ont changés. Les associations défendant les Libertés des Internautes ont-elles raison alors de soulever les polémiques ? Pourquoi s'insurge-t-on de quelque chose qui a toujours existé ? Il faut garder en tête que ce qui se joue grâce à ces nouveaux moyens va en fait au-delà de ce que nous pouvions imaginer jusqu'alors. Les possibilités extraordinaires des nouveaux outils numériques font en effet basculer ce type de surveillance dans un nouveau cadre sur deux points importants. Premièrement, il faut remarquer que les technologies permettent aujourd'hui non pas uniquement de surveiller un communauté de citoyens d'où émergerait un individu suspect mais de surveiller chaque individu de la communauté et chaque personnalité à travers ses activités quotidiennes.

Deuxièmement, il faut mesurer que devant les enjeux de cette mine d'informations à récolter, les technologies évolueront vers une meilleure capacité de stockage et un meilleur traitement en temps réels de ces informations et de ces data, transformant véritablement le concept même de «l'internet» en un centre géant de récolte de donnée alimenté par nos objets connectés : c'est l'internet des objets[1] et du big data.

• Si l'espionnage existe depuis tant d'année, c'est qu'il permet un véritable avantage : celui de tout connaître d'autrui. Cela permet d'avoir un avantage sur lui, de pouvoir cibler et agir sur ses faiblesses. L'espionné lui, se retrouve donc en position d'infériorité, plus facilement manipulable par celui qui sait sur quels points s'appuyer pour arriver à ses fins. Ce dont il s'agit ici serait donc une sorte de manipulation de l'internaute à son insu.

¶ Dans le cas d'une pratique marketing traditionnelle qui fonctionne aussi sur le renseignement, on ne parle pas d'espionnage car elle concerne un échantillon de personne, un groupe arrêté d'individu. Ce qui intéresse n'est pas la personnalité intime de chaque client potentiel mais plutôt la convergence de caractéristiques qui détermine « le marché » ou « le public » d'une action de communication publicitaire. Or avec l'arrivée de ces nouveaux outils informatiques, on remarque un nouveau type de marketing lié aux technologies de l'information : le data-mining (exploration des données) permettant le microtargetting (micro-ciblage). La partie « exploration de données » repose sur des algorithmes informatiques et des méthodes de calcul statistiques complexes, qui permettent d'identifier et de cibler non plus un public type mais un modèle très précis de personnalité concernée par la recherche effectuée. On manque encore de recul pour calculer de manière certaine l'efficacité de ce genre d'algorithmes, mais plusieurs études s'accordent sur le fait que cette technique pratiquée en politique notamment par Barack Obama lors de la campagne de 2007 et 2008 aurait été un avantage certain[3]. Le vainqueur des élections a en effet bénéficié d'une structure technologique menée par des anciens salariés de Facebook, Google et Amazon ayant un rôle de communiquant en sachant exactement à qui s'adresser, quoi dire -allant même jusqu'à un message différent par habitant d'un même foyer- et quoi demander -depuis le support au suffrage, à un don monétaire, une promotion auprès des amis ou une campagne téléphonique-. Le grand enjeu ici est donc pour les personnes ayant accès aux data, d'en faire émerger des renseignements de comportement et de personnalité sur les internautes pour les comprendre individuellement et mieux orienter leur futurs choix[10]. Cela ressemble presque à de la science-fiction, pourtant les budgets de recherches et de développement de ce type d'algorithmes —en vue de prédire les comportements d'achat de chacun ou bien les évolutions de mentalité d'un individu[1]— sont les premiers révélateurs du type d'enjeux convoités par les géants de l'internet. La question qui se pose alors est celle du libre arbitre de l'internaute. Comment être libre de mes choix, de mes actes et de mes décisions quand finalement, je n'ai accès qu'aux choix que l'on attend de moi ? Le risque est bien de consentir à porter des œillères en se complaisant dans des décisions que d'autres prendraient pour nous. A moindre échelle, c'est d'ailleurs ce qui se fait via la personnalisation des recherches Google : selon les renseignements et datas que Google à de moi et de mon ordinateur personnel, ma recherche n'aboutira pas à la même hiérarchie voir aux mêmes résultats que la même recherche effectuée par mon voisin. Cette remise en question du libre arbitre et ce danger d'œillère déjà présents ne sont que les premiers effets de l'internet du big data.

¶ Il convient en effet de tenter de se projeter dans l'avenir de l'internet pour mesurer entièrement ce qui se joue derrière la question du traitement des données générées par l'internaute. En effet, le Web n'a pas une identité fixe : depuis sa première utilisation en 1980, il est devenu public dans les années 1990 et progressivement populaire sous la forme World Wide Web avant de devenir le Web 2.0 (ou Web social), caractérisée par l'émergence des plateformes de partage et la systématisation des réseaux sociaux autour de 2005. Aujourd'hui, on sait que les principaux revenus des géants du web comme Google ou Facebook proviennent des data que les internautes génèrent : elles assurent à ces entreprises des accords commerciaux et publicitaires juteux ainsi que des arguments de supériorité stratégique qui ont un réel poids économique. On peut donc, sans trop se risquer, imaginer que les principaux acteurs de l'économie du web continueront à développer les potentiels

de nos data. En regard de cela il faut prendre en compte trois circonstances : la première est l'évolution des outils numériques. On l'observe depuis l'invention du premier ordinateur il y a peine quelques dizaines d'années et elle est spectaculaire. Ainsi, si aujourd'hui les data scrutées systématiquement en temps réel par la NSA ne sont pas stockées sur les serveurs plus de trois jours par défaut —un mois à cinq ans si elles représentent un intérêt préssenti— car elles pèsent trop lourd, on peut raisonnablement penser que bientôt les serveurs ou la manière de stocker ces datas seront améliorés. On peut donc imaginer qu'un jour, les datas que chacun produits soient stockées et archivées : une banque de renseignements sur chaque citoyen qui représenterait une source de pouvoir inédite dans les mains de la personne, de l'organisme ou du gouvernement qui la posséderait. Sans compter le caractère intemporel de ces informations : un gouvernement avec de nouvelles lois pourraient utiliser votre historique de data et selon vos pratiques, vos habitudes internets, vos mails d'il y a deux ans etc. prédire si vous êtes en accord avec lui ou non, faire de vous un citoyen à surveiller plus que les autres ou même se servir de ces informations comme moyen de pression ou de contrainte. La deuxième circonstance à observer est l'arrivée imminente des objets connectés[1]. Nos smartphones et GPS ne sont que le début de cette tendance qui agite tous les chercheurs du globe. Déjà certains objets proposant une interactivité numérique nouvelle —une connexion à l'internet et donc la génération de data renseignant de nos activités— sont sur le marché : les consoles de jeu jusqu'alors indépendantes du web, les montres, certains dispositifs de volets électriques et chauffages permettant de réguler notre consommation d'énergie en ligne, mais aussi les chaussures de sport dotées de capteurs pour améliorer nos exercices. Demain ce seront nos frigos qui proposeront de gérer les aliments en stock et le réapprovisionnement via les sites web des supermarchés, ou encore nos machines à laver qui nous alerteront sur l'usure d'un vêtement non lavés selon les recommandations du vendeurs, et pourquoi ces mêmes vêtements équipés de capteurs qui seront capables de nous renseigner à tous moments sur les variables météorologiques et les dépenses énergiques de notre corps... Il est donc tout à fait envisageable qu'attirés par des services d'optimisation de tous les objets qui nous entourent pour notre propre confort, nous soyons amenés à produire une quantité vertigineuse de ces data qui révèlent tout de notre vie quotidienne et intime et qui aujourd'hui, sont accessibles à plusieurs entreprises privés et organisations gouvernementales. Enfin, une des dernières circonstances à prendre en compte est la monopolisation de pouvoir —qui se déroule actuellement— par les leaders actuels du web. Ces leaders sont souvent des entreprises privées, qui fonctionnent sur des économies de profit et pour leur propre compte. Les concurrents de ces leaders sont les logiciels libres et services open sources : ils répondent souvent à une politique de transparence et de non-profit et leur grande différence est qu'ils donnent aux internautes l'accès à leur fonctionnement interne, leur code de programmation, avec la possibilité de le modifier soi-même, de le contrôler et de partager cette modification. A l'inverse les entreprises privés restent les seuls maîtres de leur code de programmation et gardent tous contrôle sur le fonctionnement de leur technologie. C'est en leur fournissant de notre plein gré et gratuitement nos data qui les enrichissent, que nous leur donnont tout pouvoir sur l'internet[1]. Par exemple, l'entreprise Google, célèbre pour son moteur de recherche, a lancé en 2008 son propre navigateur, affrontant ceux en place depuis la popularisation du web. Suite à une progression fulgurante, son navigateur, Chrome est aujourd'hui le plus utilisé dans le monde[11] —45% du traffic internet- devant Internet Explorer en chute libre —26% pour ce navigateur installé de base et depuis l'origine sur les ordinateurs Windows— et devant le navigateur libre Mozilla Firefox —qui accuse une baisse de 10% depuis l'arrivée de Chrome— Une des projections plausibles de l'internet du futur serait alors la toute puissance de quelques entreprises privées dirigeant comme elles l'entendent le web mais aussi notre quotidien via nos objets connectés. Ces entreprises par ailleurs détentrices d'un pouvoir invisible sur les internautes grâce au stockage massif des informations les concernant tiendraient un place importante auprès des gouvernements ravis de pouvoir surveiller si facilement, largement et précisément chacun de ces citoyens. Enfin, il ne resterait qu'à espérer que ces entreprises, quasi exclusivement Américaines, n'aient toujours que de bonnes intentions et que ce pouvoir pris sur chaque citoyen du globe ne se retourne pas contre lui-même ou contre une communauté.

¶ Il est difficile évidemment de se projeter dans la convergence de ces circonstances, ajoutées à celles que nous ne pouvons pas imaginer ; mais ce que nous pouvons entrevoir c'est le fait que les questions de « respect de la vie privé », « de libre arbitre » et de prise de pouvoir sur les internautes qui se posent dès aujourd'hui ne sont que la partie visible de l'iceberg et vont prendre une dimension colossale dans les années à venir[12].

¶ Malheureusement, les possibilités de lutte contre cette surveillance de l'internaute sont peu prometteuses. Se couper complètement des technologies est quasiment impossible à l'heure actuelle et le sera de moins en moins car c'est aussi une manière d'attirer le soupçon des organisations qui nous surveille[1]. Se tourner vers les logiciels libres peut-être un solution à court terme, mais il parait difficile pour ce type de service de non-profit de rester en compétition avec des entreprises aux moyens quasi illimités. Se tourner vers une protection de nos data par notre Etat face à cette tendance d'omnipotence des Etats-Unis parait peu porteur : les dirigeants politiques ne se sont pas vraiment insurgés de ces révélations d'espionnages faîtes pas Snowden[13]... en fait selon d'autres révélations de ce dernier, les services de renseignements de chaque Etat et les gouvernements aimeraient pouvoir en faire de même s'ils avaient les moyens de la NSA. De plus, la DGSE (Direction Générale de la Sécurité Extérieur en France) ainsi que les Services Secrets Français serait eux-mêmes partenaires dans un accord DGSE-NSA-GCHQ (l'équivalent Britannique de la NSA) pour livrer des stocks massifs de données en transit sur le sol français[14] provenant des câbles sous-marins par lesquels transitent les data des serveurs d'un pays aux serveurs d'un autre.

¶ Non seulement il apparait donc évident que les questions soulevés par les associations de défense des libertés des internautes sont justifiées, mais surtout qu'il y a une urgence de prise de conscience. Aujourd'hui les leaders de l'internet s'abritent avec brio derrière des services séduisants, ultra-efficaces et sans cesse optimisés pour que les internautes continuent d'utiliser ces services. Le problème est sûrement que la plupart de ces internautes n'a pas conscience des enjeux qui se cachent derrière les data qu'il génère et offre contre service à ces géants de l'économie qui deviennent occasionnellement les associés du gouvernement, tout du moins aux Etats-Unis. Il convient de noter ici que les intérêts de l'internaute ne sont pas forcément les mêmes que ceux des institutions gouvernementales de renseignement et des leaders de l'internet. Toute la difficulté est d'ensuite arriver à se projeter pour pouvoir choisir, aujourd'hui, de manière éclairée, notre propre utilisation de l'internet. L'urgence reste donc sûrement de faire prendre conscience à chaque internaute ce qui se joue à chaque fois qu'il ouvre son navigateur internet pour permettre l'avancé d'un débat essentiel qui laisse indifférent encore beaucoup d'internautes et de figures politiques, notamment en France.

Aliénor Fernandez, 21.12.2013

- Rappel de faits : les sources.

0. Ce soir (ou jamais !), [émission télé],
Frédéric Taddeï avec Jéremie Zimmermann, Jacques Attali, Flore Vasseur, Daniel Schneidermann, Gilles Babinet, Ellen Wasylina, Pierre Conesa, Louis Caprioli, Laurent Alexandre, Katell Auguié et Mats Carduner.
« Etats, entreprises, particuliers : tout le monde espionne tout le monde ? », 25.10.2013.
< http://www.youtube.com/watch?v=xQDYnxKiPd >

1. Michaël Szadkowski et Damien Leloup, LeMonde.fr [site web]
«Prism, Snowden, surveillance : 7 questions pour tout comprendre», 02.07.2013. Consulté le 12.12.2013
< http://www.lemonde.fr/technologies/article/2013/07/02/prism-snowden-surveillance-de-la-nsa-tout-comprendre-en-6-etapes_3437984_651865.html >

2. Martin Untersinger, LeMonde.fr [site web]
«Prism, un accès privilégié aux serveurs des géants de l'Internet», 22.10.2013. Consulté le 30.11.2013
< http://www.lemonde.fr/international/article/2013/10/22/prism-un-acces-privilegie-aux-serveurs-des-geants-de-l-internet_3500804_3210.html >

3. Glenn Greenwald, TheGuardian.com [site web]
« XKeyscore: NSA tool collects 'nearly everything a user does on the internet», 31.07.2013. Consulté le 30.11.2013
< http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data >

4. TheWashingtonPost.com [site web]
«How the NSA is tracking people right now». Consulté le 30.11.2013
< http://apps.washingtonpost.com/g/page/national/how-the-nsa-is-tracking-people-right-now/634/ >

5. Yves Eudes et Nicolas Chapuis, LeMonde.fr, [site web]
«Espionnage de la NSA : Une ligne rouge a été franchie pour la CNIL» 24.10.2013. Consulté le 30.11.2013
http://www.lemonde.fr/international/article/2013/10/24/affaire-prism-une-ligne-rouge-a-ete-franchie-denonce-la-cnil_3501948_3210.html

6. LeMonde.fr [site web]
«Aux Etats-Unis, une nouvelle action en justice contre la NSA sur l'espionnage» 16.07.2013. Consulté le 30.11.2013
< http://www.lemonde.fr/technologies/article/2013/07/16/aux-etats-unis-une-nouvelle-action-en-justice-contre-la-nsa-sur-l-espionnage_3448612_651865.html >

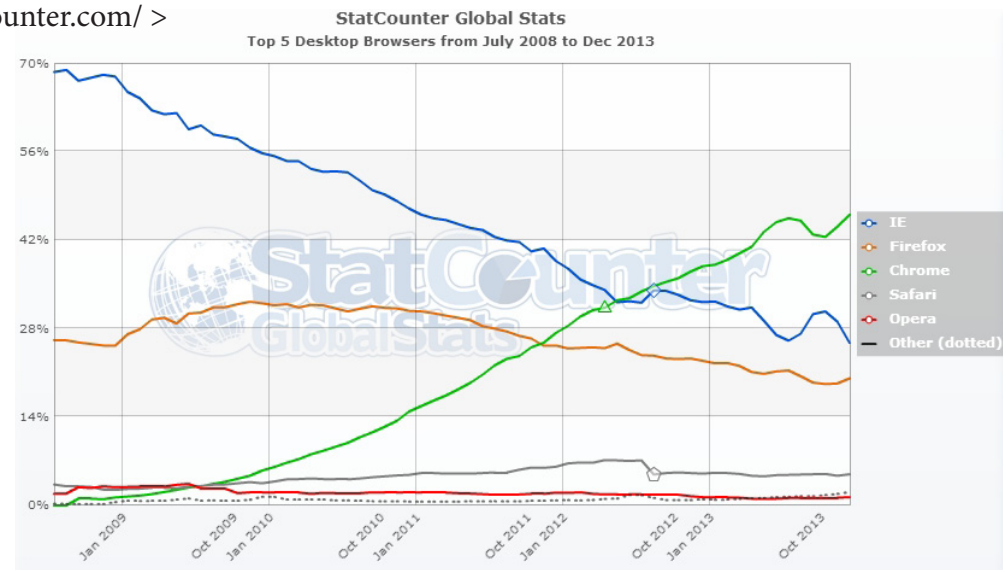
7. Jérôme Thorel, TV5Monde, [site web]
«Londres et ses poubelles intelligentes : les limites de la société de surveillance» 15.08.2013. Consulté le 30.11.2013
< http://www.tv5.org/cms/chaine-francophone/info/Les-dossiers-de-la-redaction/ACTA/p-26110-Londres-et-ses-poubelles-intelligentes-les-limites-de-la-societe-de-surveillance.htm >

9. Fabien Soyez, CNETfrance.fr [site web]
«Que fait Google de vos données ?» 13.12.2012. Consulté le 30.11.2013
< http://www.cnetfrance.fr/news/que-fait-google-de-vos-donnees-39785417.htm >

3. Pascal-Emmanuel Gobry, Atlanctico.fr [site web]
«Le pouvoir du big data : Obama 1er Président élu grâce à sa maîtrise de traitement de données ?» 9.11.2012. Consulté le 16.12.2013.
< http://www.atlantico.fr/decryptage/big-data-et-obama-avait-gagne-election-americaine-grace-tendance-en-train-revolutionner-economie-pascal-emmanuel-gobry-539455.html?page=0,0 >

10. Mike Gualtieri, Forrester, [site web]
«How Obama campaign used predictive analytics to influence voters», 27.06.2013. Consulté le 16.12.2013.
< http://blogs.forrester.com/mike_gualtieri/13-06-27-how_the_obama_campaign_used_predictive_analytics_to_influence_voters>

11. GlobalStat - StatCounter [site web] Consulté le 15.12.2013.
< http://gs.statcounter.com/ >



12. LeMonde.fr, [site web]
«Pourquoi stocker toutes nos vies sur des serveurs aux Etats-Unis ?» 12.06.2013. Consulté le 15.12.2013.
< http://www.lemonde.fr/technologies/article/2013/06/12/pourquoi-stocker-toutes-nos-vies-sur-des-serveurs-aux-etats-unis_3428857_651865.html >

13. LeHuffingtonPost.fr [site web]
«Espionnage de la NSA: la France ne peut pas faire grand chose d'autre...» 21.10.2013. Consulté le 15.12.2013.
< http://www.huffingtonpost.fr/2013/10/21/espionnage-nsa-france-demande-explications_n_4134854.html >

14. Jacques Follorou, LeMonde.fr [site web]
«La France, précieux partenaire de l'espionnage de la NSA» 29.11.2013. Consulté le 15.12.2013
< http://www.lemonde.fr/technologies/article/2013/11/29/la-france-precieux-partenaire-de-l-espionnage-de-la-nsa_3522653_651865.html >