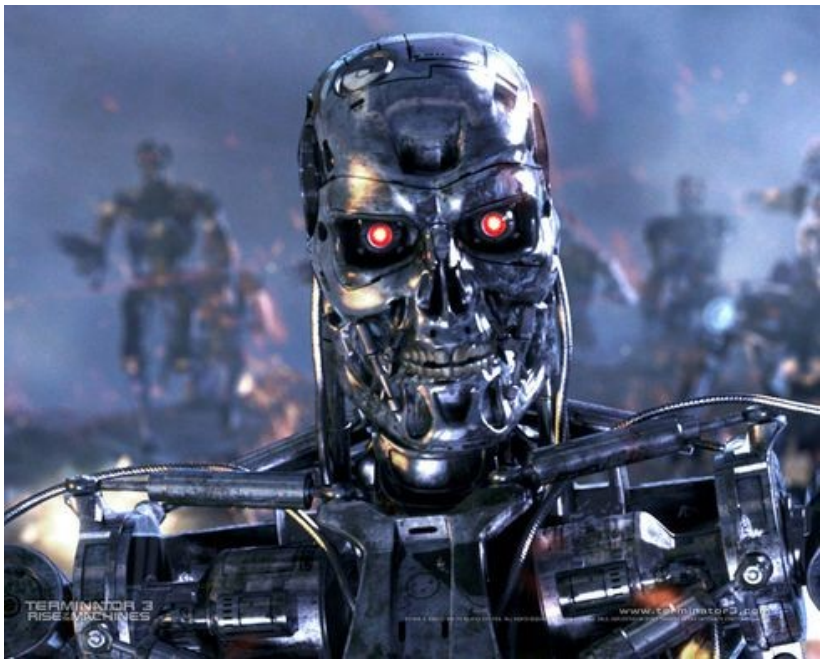
POLYTECH CLERMONT-FERRAND

Rapport de Projet Polytech

GOOGLE

PEUT-IL DEVENIR

Skynet?



Rédigé par BIAL Victoria, CAILLAUD Brice, DESPREZ Tristan, DUCHON Simon, étudiants en PeiP et dirigé par LENGAGNE Sébastien

Ce projet n'aurait pu se faire correctement sais l'aide des personnes ci-dessous que nous remercions :

Notre tuteur M. LENGAGNE Sébastien pour nous avoir orienté, conseillé et suivi tout au long de ce vaste projet.

L'école de Masage à Beaumont, ses professeurs et ses élèves CM1-CM2 pour avoir accepté de répondre à nos questions sur les technologies.
Le directeur de l'école M. BELMONT François pour avoir travaillé avec nous sur la rédaction du sondage.

L'école de Malintrat, la directrice Mme NEAU Isabelle pour nous avoir accueillie et ses élèves de CM2 pour avoir répondu à notre sondage.

La Chargée de Projet - Mise en Conformité RGPD Mme LIONNE Camille travaillant à Vialink, pour avoir répondu à notre interview sur le règlement européen RGPD.

Le professeur M. PHELIPPE Laurent pour nous avoir prêté l'enceinte connectée Alexa.

L'école Polytech Clermont-Ferrand pour le prêt de l'ordinateur Linux.

Introduction

La science-fiction est un genre artistique apparu dans la première moitié du XXe siècle, qui prends son véritable essor dans les années 70 poussé par le développement du cinéma. Ce thème est récurrent et de nombreux best-sellers voient le jour avec des projets plus futuristes les uns que les autres. C'est notamment le cas du film « Terminator », premier film à succès de James CAMERON, où l'histoire se déroule dans un futur proche où une guerre fait rage entre les humains et une intelligence artificielle appelée Skynet, qui contrôle des robots. Bien que Terminator ne soit qu'un film, nous pouvons nous demander si l'histoire racontée n'est pas en train de se dérouler sous nos yeux, sans même que l'on ne s'en rende compte. Nous sommes alors en mesure de nous demander si Google peut devenir le prochain Skynet ?

Sans réellement s'intéresser à la capacité de Google à prendre le contrôle d'une armée, nous pouvons nous intéresser sur la puissance démesurée des géants du web. En effet de nos jours, ceux qu'on appelle plus communément les GAFAM[1] ne cessent d'accroître leur hégémonie dans chacun de leur domaine, faisant d'eux des géants économiques pouvant rivaliser avec certains pays. Avec la continuelle expansion des technologies numériques dans notre société, ils ont réussi à se rendre indispensable et à garder une constante emprise sur la vie de leurs utilisateurs, notamment en ayant accès à leurs données personnelles. Même si elles se revendiquent transparentes vis-à-vis des consommateurs à travers les conditions d'utilisations, qu'en est-il vraiment ? Ces grandes firmes pourraient-elles utiliser leurs pouvoirs à des fins néfastes ?

Nous aurions pu parler de la dominance des robots et des intelligences artificielles, de comment elles auraient pu nous contrôler et imposer leur mode de vie ; mais nous avons décidé d'orienter notre sujet sur la sécurité, des limites de Google, ainsi que de notre liberté sur les réseaux.

En faisant ce choix, nous allons dans un premier temps présenter les GAFAM et leur importance dans le monde d'aujourd'hui. Nous passerons ensuite aux lanceurs d'alertes, aux techniques qu'ils ont pour nous prévenir des dangers d'Internet, quelles révélations avons-nous pus obtenir ainsi que les avancées au cours de l'histoire. Dans la continuité nous verrons quelles lois existent et en quoi elles consistent ; nous verrons aussi l'utilisation d'Internet par le gouvernement français et les GAFAM. Nous poursuivrons avec une solution pour se protéger contre la vente de nos données : le Darkweb. Puis nous finirons par deux études de cas : une sur la dépendance de l'individu aux technologies puis une autre sur le Google Home.

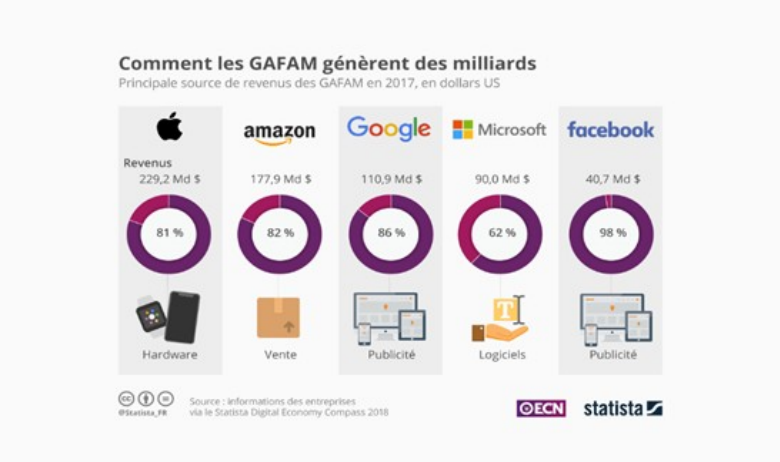
1 GAFAM: Google Apple Facebook Amazon Microsoft

Table des matières

I) Puissance économique des GAFAM

Les plus grands géants du web -- Google, Apple, Facebook, Amazon, Microsoft -- ont une puissance et un fonctionnement si proche que nous les avons associés sous un même acronyme : les GAFAM. Ils ont chacun révolutionné à leur manière l'utilisation d'internet et leurs services sont utilisés chaque jour par des internautes du monde entier. Pour comprendre leur puissance démesurée, il est important de connaître leur histoire et leur fonctionnement.

Les GAFAM se sont développés sur le marché au début du XXIème siècle parallèlement au développement d'internet dans les foyers du monde entier. Ils ont su profiter du système capitaliste international qui prône une société de consommation active pour déployer leur influence. Leurs produits sont conçus pour être indispensables et addictifs même si les consommateurs n'en ont nullement besoin et cette "économie de l'attention" fait leur force.



Comme vous le voyez ci-contre chacun à sa principale source de revenus et ils génèrent ensemble l'équivalent du PIB en Allemagne, 4e économie mondiale. Cette représentation suffit à comprendre l'ampleur de leur puissance face aux pays. Néanmoins, ces sommes astronomiques reflètent une réalité bien dangereuse pour les consommateurs ; les GAFAM sont remis en cause pour leur modèle économique car, ils collectent une masse considérable de données des utilisateurs pour les revendre aux publicitaires. Ce flux de données concerne 1.42 milliards d'utilisateurs pour Google et 2.13 milliards pour Facebook. De plus, les internautes ne peuvent pas refuser l'utilisation de leurs données personnelles tant qu'ils utilisent les services des multinationales.

Avec ce type de système, l'influence des GAFAM est très importante mondialement. Leurs services sont uniquement très limités sous les régimes autoritaires russes et chinois qui ont leur propre géant Internet. En Europe ce sont des lobbys très puissants qui imposent leur système à chaque pays au détriment des libertés individuelles ; il est extrêmement difficile de leur faire changer leur politique économique vers une politique plus éthique où l'utilisateur serait maître de ses données.

Pour sensibiliser et alerter les citoyens sur l'utilisation et la diffusion de nos données, des personnes appelées les lanceurs d'alerte ont eu le courage de dénoncer leur pratique et de les remettre en question.

II) Les lanceurs d'alertes

La société actuelle tend de plus en plus à ranger tous les individus qui la composent dans des cases, les associer à des fichiers regroupant leurs habitudes de vie ou leurs envies. Pour cela de grandes entreprises vont stocker nos données personnelles et se les échanger, parfois sans demander l'avis des personnes en question. Tout ce système se fait bien souvent à l'abri du regard du grand public, car à l'époque actuelle, le stockage de données personnelles est sujet à de grandes controverses. Certaines personnes appelées les « lanceurs d'alerte » détiennent ce genre d'informations et vont les dévoiler au grand jour car elles estiment qu'elles sont dangereuses pour la société. Ils ont dévoilé en seulement quelques années des centaines de scandales et de secrets d'Etat mais dans le cadre de ce projet nous ne nous intéresserons qu'à ceux qui touchent à l'espionnage de notre vie privée ou encore au stockage de nos informations personnelles.

1. Qu'est-ce qu'un lanceur d'alerte ?

Les lanceurs d'alerte sont des individus qui vont révéler des informations qu'ils estiment dangereuses ou illicites, un état de fait qui menacerait les droits des hommes, l'écologie, ou encore la vie privée.

Voici la définition que le Conseil européen a fait des alertes : « l'alerte concerne la révélation d'informations sur des activités qui constituent une menace ou un préjudice pour l'intérêt général. Les personnes lancent une alerte car elles considèrent qu'il doit être mis fin à ces activités ou que des mesures palliatives doivent être prises. Souvent il s'agit simplement d'informer les employeurs des agissements irréguliers dont ils ignorent l'existence et qu'ils s'empressent de corriger. Dans d'autres cas, les lanceurs d'alerte peuvent estimer nécessaire de contacter les organes réglementaires ou de contrôle, ou les autorités de répression compétentes.
Parfois les lanceurs d'alerte voudront rendre publics ces actes répréhensibles, le plus souvent par le biais de l'internet et d'autres médias, ou en contactant des groupes de défense de l'intérêt général ou des parlementaires ».

A la différence d'un détracteur, un lanceur d'alerte doit en théorie dénouer de mauvaises intentions et n'a pas pour but de générer une révolution, de la peur, ou d'attirer l'attention sur lui-même.

Les lanceurs d'alerte sont bien plus présents que ce que l'on peut entendre sur les réseaux.
En effet puisque les fraudes et les limites des droits humains se font à travers le monde entier, les lanceurs d'alerte sont présents dans chaque pays, même si certains pays présentes beaucoup plus de risques que d'autres.

Les lanceurs d'alerte existent depuis un demi-siècle, le premier est apparu en 1971.
Daniel Ellsberg était analyste militaire pour la RAND corporation avant de dévoiler des secrets militaires sur la guerre du Vietnam dans la presse, histoire qui sera plus tard reprise par Spielberg pour réaliser Pentagone Papers. Puis Daniel Ellsberg fut conduit en justice pour vol, conspiration et espionnage. Il sera également présenté comme un traître dans tous les médias mais il obtiendra finalement en 2006 le prix Nobel alternatif.

Après cette première apparition les cas de lanceurs d'alerte sont de plus en plus fréquents malgré les potentiels risques. En effet les lanceurs d'alerte risquent beaucoup en dévoilant une information, il menace leur sécurité financière et physique, leurs couple et familles, leur identité est dévoilée. Les lanceurs d'alerte peuvent être traités de traître par l'Etat, perdre leur travail et sont souvent victimes de poursuites bâillons[1].

2. Des protections pour les lanceurs d'alertes ?

Les lanceurs d'alerte permettant des changements considérables dans plusieurs domaines notamment la corruption, il est donc indispensable qu'ils soient protégés par la loi contre toutes représailles. De plus le droit d'alerte peut être considéré comme une extension du droit d'expression.

Dès 2004 certains organismes comme Transparency International se sont chargés de faire avancer la protection des défenseurs des droits et ce n'est que récemment, le 9 décembre 2016 que la loi n°2016-1691 relative à la transparence, à la lutte contre la corruption et la modernisation de la vie économique est adoptée. Cette dernière garantie la sécurité du défenseur des droits, une irresponsabilité pénale, la non-divulgation de l'identité, la nullité des représailles et une réintégration de l'emploi. Cependant pour que le lanceur d'alerte puisse bénéficier de cette protection il doit respecter trois étapes.

- Étape 1 : Alerter en interne
  Le lanceur d'alerte doit saisir en premier lieu la voix interne, tout supérieur hiérarchique direct ou indirect, l'employeur ou le référent indiqué par l'employeur.
- Étape 2 : Alerter l'autorité compétente
  Si l'alerte n'a pas été traitée dans un délai raisonnable, le lanceur d'alerte doit s'adresser aux autorités judiciaires, administratives ou professionnelles compétentes.
- Étape 3 : Alerter publiquement
  Si l'alerte n'a pas été traitée dans un délai de 3 mois, le lanceur d'alerte a le droit de la rendre publique à travers les médias, les ONG, les syndicats.

En cas de danger considéré comme étant grave ou imminent, le lanceur d'alerte peut passer directement au palier 2 ou 3 en fonction du niveau de gravité de l'alerte.

Le lanceur d'alerte peut également contacter des organisations telle que « Les défenseurs des droits » pour être guidé en fonction de l'alerte, pour suivre la procédure et contacter les autorités concernées par la situation.

Une seconde option pour un lanceur d'alerte est de demander l'asile politique. En effet depuis la déclaration des droits de l'homme de 1948, l'article 14 stipule que devant la persécution, toute personne a le droit de chercher et de bénéficier de l'asile dans d'autres pays. C'est pourquoi certains lanceurs d'alerte particulièrement important ont été accueillis par d'autres pays pour garantir leur sécurité. Par exemple on pourrait citer les célèbres Edward Snowden et Julian Assange vivant respectivement en Russie et en Équateur. Cependant ces asiles sont souvent temporaires et ne règlent pas tous les problèmes tels que la protection de

1Poursuites bâillons : procédures qui ont pour objectif de censurer et dégrader l'image de l'individu.

l'anonymat ou les sanctions pénales. De plus les pays n'accordent pas le droit d'asile à tous les cas de lanceurs d'alerte.

Les solutions alternatives sont les célèbres sites Cryptome.org ou Wikileaks[1]. Ce dernier permet à n'importe qui de publier des documents publiquement et anonymement sur le site.

Le site ayant pris de l'importance très rapidement les révélations les plus importantes sont ensuite vues et relayées par de grands médias tels que le New York Times. Cette alternative sert de tampon entre les internautes et la presse pour préserver l'authenticité de l'information et l'anonymat des personnes concernées.

Le site passant par le network « Tor », il est très difficile d'intercepter l'identité et la localisation de l'émetteur des documents ce qui permet une meilleure sécurité. Néanmoins Wikileaks ayant divulgué plusieurs millions de documents et fait éclater de nombreuses polémiques aux plus hauts niveaux s'est retrouvé à de nombreuses reprises face à des problèmes techniques et financiers importants ; le site a failli être supprimé plusieurs fois, en 2011 toutes les banques du monde ont créé un blocus financier contre Wikileaks.

On peut donc affirmer que depuis quelques années les solutions pour protéger les lanceurs d'alerte se sont multipliées même si actuellement elles ne garantissent toujours pas une protection optimale. Le choix de faire partie des lanceurs d'alerte reste encore à notre époque compliquée car c'est un statut présentant de nombreux risques.

Les informations que nous cherchons dans notre projet visant à déterminer si « Google peut devenir le prochain Skynet » ne sont pas objectives et se basent que sur des rumeurs plus ou moins fondées.

Mais grâce aux lanceurs d'alerte nous pouvons avoir accès à plusieurs révélations à propos de l'espionnage de masse ou le stockage de nos données personnelles.

3. Alertes sur l'espionnage

Edward Snowden était un employé qui travaillait comme analyste de données confidentielles au compte de l'état américain à la NSA[2] et a dévoilé le 6 juin 2013 le programme de surveillance de citoyen d'entreprise et d'état nommé « PRISM ». Ce programme explique les méthodes et pratiques qu'utilise la NSA pour surveiller les données privées.

Il suffirait d'un simple soupçon, une simple recherche un peu suspecte dans une barre de recherches pour se retrouver immédiatement tracé par l'état. Il a dit lui-même « la NSA ment systématiquement au congrès quant à l'ampleur de sa surveillance aux États-Unis ».

D'après les informations sur Wikileaks les sommes versées par les pays dans l'espionnage

1 Wikileaks est une organisation non gouvernementale créée en 2006 par Julian Assange qui publie de nombreux documents confidentiels.

s'élèvent à plusieurs millions voir plus, avec en première place les Etats-Unis pour un budget estimé à 14,7 milliards de dollars. La première puissance mondiale est de loin la plus dangereuse ; 107 000 employés sont utilisés pour surveiller les citoyens et les autres pays, soit plus que la multinationale Total. L'Europe se situe loin derrière mais attribue tout de même un budget considérable à l'espionnage notamment l'Angleterre qui est la deuxième puissance mondiale dans ce domaine. Maintenant il est difficile de connaître toute l'ampleur de la surveillance de masse, nos seules connaissances se limitent à ce que nous disent les lanceurs d'alerte sur le sujet.

Un autre lanceur d'alerte du nom de Felix Krause, un développeur autrichien, dénonce en octobre 2017 l'accès trop simple à la caméra des smartphones plus particulièrement chez Apple. A titre d'exemple Felix Krause a créé un faux site de rencontres nécessitant pour la première utilisation une photo de profil et donc un accès à l'appareil photo. A partir de là Felix Krause peut prendre des photos ou des vidéos par la caméra avant et arrière à l'insu de l'utilisateur, même si l'application est mise en tâche de fond. Des propositions simples ont été faites pour régler le problème comme une simple LED qui s'allume lorsque la caméra marche. Même si cela révèle du bon sens et d'un meilleur respect de la vie privée, Apple a constamment rejeté toutes propositions sans arguments.

Un lanceur d'alerte employé chez Google resté anonyme explique comment fonctionne la multinationale. La source de revenus principale vient des publicités, leur priorité est donc de présenter les publicités les plus ciblées possibles aux utilisateurs. Pour cela Google va pour chacun d'entre nous créer un profil dans ses serveurs à l'aide de 3 règles simples :

Dis-moi qui tu fréquentes, je te dirai qui tu es. En effet Google a besoin de connaître nos fréquentations pour mieux comprendre l'individu. Pour cela l'entreprise utilise nos amis Facebook, le pillage de nos données smartphones ou encore la géolocalisation. Google via nos box Wi-Fi et nos connections internet peut savoir où nous nous trouvons à chaque instant, ce qui est le meilleur moyen de savoir quelles sont nos fréquentations potentielles et nos activités régulières.

Dis-moi de quoi tu t'occupes, je te dirai ce que tu deviendras.
Le meilleur moyen de nous délivrer les bons messages publicitaires est de savoir près de quel magasin, quel événement on est à travers encore une fois la géolocalisation. Il est également utilisé les milliers de réseaux nous demandant de laisser des « j'aime » sur ce qui nous intéresse de près ou de loin. Ces « j'aime » que l'on dépose sur Facebook, Instagram, Twitter ou Youtube servent avant tout à cerner notre caractère et notre personnalité.

Délivrer le bon message publicitaire, à la bonne personne, au bon moment, par le bon canal. Tous ces éléments servent finalement à délivrer le message publicitaire qui pourrait potentiellement susciter notre attention. La principale source de revenus du web gratuit reposant sur la publicité, Google espionne tous ses utilisateurs.

4. Espionnage de masse et stockage des données personnelles

2 La NSA, National Security Agency est une organisation gouvernementale chargé de la défense des Etats-Unis.

Avec autant de données personnelles recueillies sur chaque individu par les entreprises comme Google, Facebook … Certaines organisations deviennent particulièrement dangereuses pour notre vie privée.

Prenons l'exemple de la géolocalisation téléphone. Nous savons que le téléphone est géolocalisable s'il est connecté à un compte Google et qu'il est possible d'activer son emplacement depuis un ordinateur si le téléphone est allumé. Actuellement il est possible de faire bien d'autres choses grâce à un compte Google depuis un ordinateur à un téléphone comme désynchroniser le téléphone ainsi que son compte par exemple. Mais depuis un téléphone éteint et donc sans énergie, il ne serait pas possible que le téléphone soit géolocalisable. En effet, quand un appareil mobile utilisant l'OS Android est éteint, il n'existe pas d'élément de l'OS qui reste activé ou émet un signal. Google ne peut pas allumer un terminal à distance" d'après Google. Nokia valide ce propos en disant qu'il n'existe pas de terminaison ou de malware permettant de réactiver ces composantes lorsque le téléphone est éteint. On a pourtant découvert qu'il existe une méthode nommée "the find" que la NSA utiliserait afin de géolocaliser les téléphones éteint. Il l'aurait utilisé en Irak lors d'Al-Qaïda.

La plus importante des organisations en terme d'espionnage reste d'ailleurs la NSA. C'est l'organisme gouvernementale en charge de la sécurité des systèmes d'informations du gouvernement américains, on pourrait la résumer à une cyber-armée américaine. La NSA a deux missions : la protection de la sécurité des systèmes de communications des Etats-Unis et l'écoute de leurs ennemis. L'organisation est survenue après les attentats du 11 septembre 2001 lorsque l'ennemi pouvait être partout. Après les révélations d'Edward Snowden, il s'avère que cette lutte anti-terroriste n'a jamais réellement était une priorité mais plus un moyen de pouvoir faire de la collecte d'informations en masse.

Pour le moment nous ne connaissons que deux programmes de la NSA :

- La surveillance ciblée. Cela consiste à utiliser tout le matériel et toutes les méthodes possibles pour infiltrer des réseaux dangereux. C'est ce pour quoi la NSA a été créée et c'est ce qui lui est demandé.
- La surveillance en « vrac ». Cette partie est celle qui atteint notre vie privée puisqu'elle consiste à intercepter toutes les communications (appels, mails, SMS …) possibles sans discernement entres les individus. Ces métadonnées sont ensuite stockées et peuvent être réutilisées n'importe quand, elles n'aident pas à la sécurité des citoyens et peuvent simplement les mettre en danger si elles sont divulguées à une personne physique ou morale malveillante.

Actuellement il n'y a pas que des opposants à la surveillance de masse ; une partie de la population non-négligeable (17%) est favorable. De plus certaines personnes estiment qu'il est impossible de pouvoir mettre en place un tel système de surveillance qui coûterait bien trop cher soit 6 milliards d'euros sur 10 ans. D'après certaines personnes qualifiant la surveillance de masse de « paranoïa généralisée » les services de renseignements ne peuvent espionner en temps réel l'intégralité de la population mais ne font que stocker et analyser les données des N+2 personnes en lien avec une cible. Par exemple vous serez écouté si vous communiquez avec quelqu'un qui communique avec une cible.

Chaque jour on en apprend un peu plus sur ce que pourrait être la surveillance de masse mais il ne faut pas oublier que nous n'en serons certains que lorsque les acteurs de ces espionnages feront des révélations publiques. En attendant nous ne pouvons que nous protéger du mieux que nous le pouvons.

5. Peut-on limiter la surveillance de masse ?

Il est possible de faire valoir nos droits et d'agir individuellement pour protéger nos données personnelles. Quelques mesures permettront de limiter dans un premier temps les informations qui vous sont prises.

- Installer un pare-feu (firewall) récent pour éviter des logiciels espions d'intégrer votre ordinateur.
- Trier les cookies qui permettent aux sites visités de garder en mémoire nos identifiants, notre navigation à travers le site et autres informations indispensables au fonctionnement économique de ces derniers. Les cookies sont utilisés sur la très grande majorité des sites web et sont parfois obligatoires pour y accéder. Il est possible de les supprimer et il est conseillé de le faire fréquemment.
- Supprimer les historiques de navigation pour limiter le traçage des habitudes de vie.
- Faire attention aux forums et réseaux sociaux, tous les éléments de votre vie privée deviennent publics.
- N'accepter pas de service de géolocalisation pour éviter à Google de vous tracer.

Face à Google, d'autres moteurs de recherche proposent des alternatives pour un meilleur respect de la vie privée, on peut citer :

- The Onion Router qui rend anonyme l'utilisateur. Le résultat visible est que les publicités ne sont plus ciblées.
- Mozilla Firefox « Optimize Google » qui permet de rendre anonyme le cookie Google, empêche l'outil d'analyse de Google « Google Analytics » de récolter des statistiques sur l'utilisateur et supprime les publicités (comme Adblock Plus).
- Lilo qui, en plus de proposer à l'utilisateur de soutenir une cause précise lié à la santé, l'environnement ou le social, ne sauvegarde pas nos données.
- Scroogle, un logiciel qui détourne la récolte de nos données de Google ; il lui fournit une nouvelle adresse I.P. à chaque recherche, et accepte l'installation du cookie sur son serveur avant de le supprimer.

En conclusion on peut dire que les seules informations pour démêler le secret de la paranoïa nous proviennent des lanceurs d'alerte. Grâce à eux nous pouvons imaginer ce que peut être l'espionnage de masse et essayer de s'en protéger. En France ce n'est pas autant développé mais aux Etats-Unis l'espionnage est vu comme une de leur priorité et beaucoup de pays tentent de les égaler. Pour le moment nous ne connaissons pas encore tous les dangers qui nous entourent (en termes d'informations virtuelles) mais sûrement que dans quelques années de nouveaux scandales apparaîtront sur Wikileaks pour nous effrayer un peu plus.

II. Réglementations

1. Différentes lois mises en place par le gouvernement français

Depuis 2004, plusieurs lois ont été mises en place par le gouvernement français pour encadrer le web français. Certaines lois sont accées sur de sévères sanctions en cas de téléchargements illégaux (Hadopi), l'encadrement du commerce en ligne et le blocage de tous types d'activités pédopornographiques. Nous voyons ci-dessous 3 lois mises en place pour renforcer l'accès aux données personnelles informatiques et lutter contre la criminalité organisée ainsi que le terrorisme mais elles se sont fait critiquer en raison de l'atteinte aux libertés publiques et à notre vie privée.

- Loi Perben 2 en 2004 :

Du nom du garde des sceaux de l'époque, cette loi vise à réduire les délinquances et la criminalité organisée en surveillant la communication sur internet. Elle renforce les pouvoirs policiers aux dépens de ceux de la justice ainsi certaines actions sont exécutées sans l'accord d'un juge (dispositifs d'écoute par exemple). Par ailleurs les personnes sanctionnées ne sont pas clairement ciblées : créateur du site, hébergeur ou auteur de la publication, cela n'est pas fixé et reste trouble d'un point de vue juridique.

- Loi LPM en 2016 :

Autrement dit la Loi de Programmation Militaire fixe le budget de l'Etat pour ses forces armées sur les 3 à 6 prochaines années. En 2013, la loi admet un budget conséquent pour la cybersécurité et autorise l'accès des services de renseignements intérieurs aux réseaux téléphoniques et informatiques de ses citoyens.

- Loi sur le renseignement 24 juillet 2015 :

Les attentats de Charlie le 7 janvier 2015 ont accéléré la mise en place de cette loi. Elle permet de détecter les comportements suspects à partir des connexions personnelles en temps réel, contrairement à avant. Ces pratiques étaient déjà utilisées par les services de renseignements français mais cette loi permet de légaliser ces pratiques et de simplifier les procédures judiciaires. Les deux organisations mises en place par l'Etat pour surveiller ces données sont la Direction Générale de la Surveillance Extérieure (DGSE) et la Direction du Renseignement Militaire (DRM).

Ces détections sont faites à travers des algorithmes installés dans des boîtes noires placées au sein des Fournisseurs d'Accès Internet dit FAI. Les FAI ont accès à toutes nos données et sont responsables du contenu disponible sur internet. Ils doivent par exemple supprimer tous les sites faisant l'apologie du terrorisme. Nous pouvons citer parmi les FAI les plus connus Orange, Free, Bouygues ou SFR.

Les boîtes noires sont officiellement actives depuis octobre 2017 selon l'organisme indépendant de la Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR). La CNCTR surveille les organisations en charge du renseignement et leurs usages des boîtes noires. Selon le président de la CNCTR Francis Delon, il y a eu un « long travail » avec le gouvernement pour examiner l'algorithme et évaluer sa finalité, la lutte contre le terrorisme. Sur l'algorithme lui-même, la CNCTR a établi plusieurs modifications après un « contrôle technique très poussé ».

Les métadonnées analysées par l'algorithme sont toutes les données techniques accompagnant une connexion excepté le contenu du message ; c'est-à-dire quels sites ont été visités par une adresse IP, à quelle heure, si un message a été envoyé sur Facebook, Gmail, à quelle personne, quelle recherche a été effectuée sur Google, etc.

Les données relatives au fonctionnement de l'algorithme sont publiées dans un décret non-public et classifié. Nous ne pouvons donc pas savoir à partir de quand nous sommes surveillés, c'est un traitement automatisé. Par ailleurs la levée de l'anonymat d'une personne suspectée ne se fait qu'en cas de révélation d'une menace terroriste et sur ordre du Premier ministre (ainsi que de l'avis de la CNCTR).

Néanmoins les opposants font remarquer une atteinte à la vie privée à cause de cette loi pouvant s'appliquer à des personnes non concernées par le terrorisme. Elle s'applique à toute « personne préalablement identifiée susceptible d'être en lien avec une menace » ainsi que les « personnes appartenant à l'entourage de la personne concernée par l'autorisation [de surveillance] ». Ainsi une quantité importante de personne en France peut être surveillée suite à cette loi ; il suffit d'être lié au troisième degré de séparation à un suspect pour être soi-même suspect. Pour ces personnes, le contrôle en temps réel de toutes leurs métadonnées peut être réalisé.

C'est pourquoi des dizaines d'associations et de syndicats tels que Human right Watch, Amnesty international, RSF, CGT police considèrent ce projet de loi comme inquiétant pour les libertés individuelles en permettant une surveillance abusive. Comme le disait Benjamin Franklin, " un peuple prêt à sacrifier un peu de liberté pour un peu de sécurité ne mérite ni l'une ni l'autre, et finit par perdre les deux".

Le principal flou juridique de toutes ces lois tourne autour des personnes suspectées et potentiellement coupables. En effet on ne sait pas réellement quels sont le nombre d'individus surveillés et ceux réellement coupables mais on peut logiquement penser que c'est une surveillance de masse au vu des suspicions qui peuvent facilement s'exercer sur un citoyen lambda.

2. Les GAFAM

Les GAFAM quant à eux récoltent les données personnelles de l'utilisateur pour des raisons tout à fait différentes du gouvernement, elles sont principalement commerciales. Le modèle économique de Google, Facebook et autres services gratuits pour l'utilisateur repose

exclusivement sur la publicité. Ils développent leur puissance économique grâce à la collecte des informations personnelles des utilisateurs revendues ensuite à des publicitaires, afin de mieux cibler leur profil. Beaucoup de reproches sont faits aux GAFAM c'est pourquoi, à travers les critiques et procès ayant entachés Facebook, nous allons cerner les lacunes en matière de protection de données personnelles.

Un gigantesque scandale a éclaté en mars 2018 mettant en cause la protection de données personnelles. Le scandale vient de Cambridge Analytica, une entreprise ayant apporté un soutien indirect au président Trump. Grâce à leurs 253 algorithmes analysant et stockant les recherches et j'aime sur Facebook, l'entreprise pouvait connaître la vie privée de l'utilisateur et lui afficher des messages le touchant émotionnellement, permettant ainsi de modifier son jugement sur l'élection, en faveur de Trump. Facebook avait relevé ce problème mais n'en avait pas tenu informé les individus visés pensant que « les données avaient été détruite » par Cambridge Analytica. Cette manipulation de masse a pourtant atteint près de 87 millions de personnes.

La firme est aussi remise en cause car d'après les révélations de Christopher Willie, ancien directeur de recherche de Cambridge Analytica, une quantité impressionnante d'informations peut être disponible pour une campagne publicitaire à travers Facebook et celles-ci permettent d'établir le profil psychologique de l'individu visé. Entre autres, il y a les boutons « j'aime » et « partager » qui établissent notre profil et nos préférences. D'ailleurs selon le cofondateur de la *Quadrature du Net*, Benjamin Sonntag : « Avec 100 clics, Facebook nous connaît mieux que notre famille. Avec 250 clics, il nous connaît mieux que notre conjoint » et tout ça grâce à un algorithme très perfectionné. Les cookies utilisés n'y sont pas pour rien car ce sont des fichiers permettant de faire le lien entre un site et Facebook afin d'identifier et rassembler nos envies. Enfin toujours selon Christopher Willie, une personne n'ayant pas de compte Facebook à quand même un « profil fantôme » pour enregistrer ses données et connaître ses envies, ses besoins.

Facebook étant fautif à ne pas protéger les données de ses utilisateurs et aussi pour avoir laissé Cambridge Analytica agir, son PDG Mark Zuckerberg est passé plusieurs heures devant le Congrès américain et la Chambre des Représentants pour répondre aux questions sur la politique de confidentialité de Facebook. Le résultat des auditions a été peu convaincant car il n'y a jamais eu des réponses claires aux questions précises telles que la responsabilité de Facebook dans l'affaire, la surveillance des applications disponibles sur la plateforme, la future régulation envisagée pour faire face à ce type de problèmes… Zuckerberg s'est principalement

excusé sur des problèmes maintes et maintes fois pointés du doigt. En effet depuis la création de Facebook en 2004 la firme a déjà dû s'expliquer pour des évènements remettant en cause la sécurité de ses utilisateurs ou pour soutenir une idéologie ou une tendance politique. Parmi les plus connus on peut citer :

-L'affaire Snowden : en 2013 pour donner suite aux révélations d'Edward Snowden, la collaboration entre Facebook et la NSA (Agence Nationale de la Sécurité) susmentionnée éclate au grand jour.

-En 2014 malgré les lois précédemment établies en Europe, Facebook a aussi eu des problèmes autour du consentement libre. Les utilisateurs ne pouvaient pas accéder à ses filiales (Instagram et WhatsApp) s'ils n'acceptaient pas les conditions. Facebook a aussi été responsable d'une correspondance automatisée entre les comptes de leur groupe et WhatsApp. Comme la Commission européenne n'a pas été tenue au courant de cette nouvelle correspondance elle a déclaré avoir reçu un « renseignement inexact et dénaturé ». Etant donné que la Commission a la possibilité d'infliger 1% du chiffre d'affaire de l'entreprise, le 18 mai 2017 Facebook a reçu une amende cent-dix millions d'euros.

-En mai 2017, selon le journal britannique The Guardian, des modérateurs Facebook a reçu pour instruction de tolérer les postes négationnistes et contestant la véracité de la Shoah alors qu'il va de sa responsabilité de plateforme médiatique de modérer, voire d'interdire certains propos incitant à la haine et à la violence.

-Depuis août 2017 des millions de Rohingyas ont fui la Birmanie et les violences infligées par une certaine partie de la population pour se réfugier au Bangladesh. Selon des experts des droits de l'Homme des Nations unies, Facebook a eu "un rôle déterminant" dans la propagation de discours de haine ultra-nationaliste relayés sur sa plateforme et lus par des millions de Rohingyas.

Grâce à des logiciels qui affichent les traceurs de certaines firmes (Google et Facebook en font à chaque fois partis), nous savons que nous sommes suivis sur chaque site visité comme vous pouvez le voir ci-dessous avec Marmiton, Blablacar et Le Monde. Nous avons utilisé Avast et nous remarquons que les traceurs permettent aux entreprises de connaître nos recherches, quel site on apprécie, à quoi on s'intéresse. Les personnes ciblées en sont rarement informées ou leur consentement n'est pas obtenu. Facebook se dédouane de cette responsabilité en la faisant peser sur les sites et applications ayant intégré leur traceur. Bien que ces sites et applications soient bien responsables juridiquement, Facebook l'est tout autant. En 2017, la Commission Nationale de l'Informatique et des Libertés française (CNIL) l'a condamné à 150 000 € d'amende pour "absence d'information claire et précise concernant la collecte des données de navigation des internautes".

3. Le RGPD

Le RGPD, Règlement Général sur la Protection des Données, est mis en place à compter du 25 mai 2018 par la Commission européenne pour encadrer les entreprises et les sites sur l'utilisation de nos données personnelles. Ce règlement en remplace un bien plus ancien datant de 1995 qui ne prenait évidemment pas en compte les problématiques actuelles. Il permet aussi d'uniformiser toutes les différentes lois qu'il y avait au sein des vingt-huit pays de l'Union Européenne.

En France la CNIL[1] est l'autorité indépendante qui veille au bon fonctionnement du RGPD et aux sanctions encourues en cas de non-respect. Son but est que l'informatique reste au service du citoyen. Pour développer cette partie nous avons interviewé Camille Lionne, chargée de projet de Vialink pour la mise en conformité RGPD. Un membre de Vialink était idéal pour nous renseigner car l'entreprise travaille précisément sur la mise en place de processus sécurisés 100% numériques.

- Applications du règlement et avancées

Le RGPD renforce et éclairci des principes déjà applicables auparavant, nous allons examiner ci-dessous les avancées. Pour les plus grandes entreprises comme les GAFAM, le règlement européen demande une AIPD[2]. Ils doivent expliquer les détails du traitement, si l'utilisation de la base de données respecte les principes et droits fondamentaux (finalité, données et durées de conservation, information et droits des personnes) et ces compagnies analysent les risques potentiels sur la sécurité des données.

Les principes de Privacy by Design et by Default obligent les entreprises à intégrer le RGPD dès l'élaboration d'une nouvelle technologie. Le rôle de DPO, Délégué à la Protection des Données, est désormais obligatoire dans chaque entreprise, c'est celui qui fait le lien entre l'entreprise et la CNIL. Il n'est pas là pour surveiller l'entreprise mais pour lui apporter les éléments qui doivent être corrigés afin qu'elle soit en accord avec le règlement. Le DPO s'assure aussi d'une cybersécurité correcte. Si une défaillance dans la sécurité existe, le DPO à l'obligation de prévenir la CNIL mais aussi le public concerné par la potentielle menace. Pour se plier aux exigences du RGPD et ne pas avoir de sanctions, des logiciels de sécurité sont recommandés aux entreprises.

Tout traitement doit avoir une finalité prédéterminée, c'est-à-dire que les données doivent être traitées dans un but, selon un objectif clair et défini à l'avance. La personne qui traite ou fait traiter les données personnelles (appelé le Responsable de Traitement) devra tout d'abord donner un motif au traitement. Pour que le traitement des données soit légal, le RGPD définit 6 bases
légales :

- le respect d'une obligation légale, l'entreprise repose sur cette base légale pour établir par exemple le bulletin de paie des salariés.
- l'exécution d'un contrat.
- l'intérêt légitime du responsable de traitement.
- la sauvegarde des intérêts vitaux de la personne.
- l'exécution d'une mission d'intérêt public.
-le consentement, le plus controversé chez les GAFAM en raison des modalités du consentement.

La personne doit avoir été informée précisément sur ce à quoi elle consent. En l'occurrence une entreprise ne peut pas considérer qu'un individu est consentant, s'il accepte uniquement sa géolocalisation sur son mobile ou s'il se créer un compte. Pourtant lorsqu'internet et la localisation sont activés, l'utilisateur est précisément repéré. Cela permet de connaître nos envies, nos habitudes et nos trajets pour mieux tracer un individu et lui proposer

1 Commission Nationale de l'Informatique & Libertés est une autorité française établit en 1978.
2 Analyse d'Impact sur la Protection des Données

des publicités adéquates. Ce qui est moins connu est que même sans la localisation d'activer ou même internet la personne est repérée par les réseaux. Chaque téléphone ayant une carte SIM est connecté au réseau le plus proche et c'est à cause de celui-ci que la géolocalisation est automatisée.

Si l'utilisateur change d'avis, ne veux plus que les entreprises aient accès à ses données, il peut faire valoir son droit à l'effacement dit aussi droit à l'oubli. Ce droit s'exerce sous certaines conditions : lorsque les finalités pour lesquelles les données ont été collectées ne sont plus nécessaires, lorsqu'elle retire son consentement. Ce droit n'est pas toujours accordé, par exemple si ces données sont basées sur une obligation légale (les informations données auprès des finances publiques pour calculer nos impôts ne peuvent pas être supprimées).

- Sanctions

Avec le RGPD, les sanctions envers les GAFAM sont bien plus intransigeantes. Ce règlement a considérablement augmenté les plafonds de sanctions, qui peuvent désormais s'élever au maximum à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial de l'entreprise.

Le 21 janvier 2019, la CNIL a prononcé une amende de 50 millions d'euros à l'encontre de Google en appliquant, pour la première fois, les sanctions prévues par le RGPD. Cette sanction se justifie, selon la CNIL, par la gravité des manquements concernés en matière de transparence, d'information et de consentement des utilisateurs.

Pour les entreprises moins puissantes et fonctionnant à l'échelle d'un pays ou plus localement, appliquer le règlement prend plus de temps. Il y a eu en France plusieurs mises en demeure pour des sociétés qui proposent leur service de sauvegardes et d'analyses de données des utilisateurs tels que Singlespot, Vectaury, Fidzup mais elles ont toutes été en conformité avant le délai imparti par la CNIL. La CNIL reste soucieuse des efforts pris par les entreprises et va se préférer un rôle pédagogique à un rôle sanctionnateur.

Les sanctions sont encore rares, mais la plus significative reste celle adressée à l'encontre de Google, ce qui semble montrer la volonté de la CNIL de sanctionner les GAFAM plus que les entreprises de taille relative.

- Eveil des consciences

Depuis l'entrée en vigueur du RGPD, certains chiffres sont des indicateurs de la prise de conscience des personnes et des entreprises. La consultation des foires aux questions en ligne sur le RGPD a augmenté de 83%, quant aux moyens humains développés pour accompagner les entreprises, la CNIL a désigné 13000 DPO contre 5000 CIL l'année précédente.

La CNIL a recensé 11000 plaintes en 2018 de la part de particuliers ou d'associations prônant les libertés individuelles contre 8000 en 2017, ainsi que plus de 190 000 appels contre 150 000 en 2017.

- Prochaine étape : ePrivacy

Même si nous sommes très avancés en Europe avec le RGPD, le chemin est encore long pour avoir une meilleure protection des données. Avant de continuer ce combat il est nécessaire de s'assurer de la conformité des entreprises face aux réglementations actuelles.

Néanmoins un projet de règlement appelé ePrivacy vient préciser le règlement européen et renforce la protection de la vie privée dans le secteur des télécommunications. Il devait normalement être mis en place en parallèle du RGPD, il n'est donc pas annulé mais seulement

retardé. Le texte prévoit la nécessité de devoir récolter le consentement explicite des internautes avant de déposer des cookies de traçage à des fins publicitaires.

C'est notamment du fait de ce règlement en cours de validation que nous voyons apparaître un bandeau d'affichage nous demandant notre accord pour déposer des cookies de pistage sur notre navigateur « pour le bon fonctionnement du site ». Avec ePrivacy, l'utilisateur doit être libre d'accéder au site même sans son consentement, privant celui-ci de précieuses informations personnelles valorisées grâce à la publicité ciblée.

Le RGPD est d'une toute autre envergure que toutes les lois mises en place jusqu'à présent, elle remet en cause les entreprises ne respectant pas la vie privée des citoyens sur internet et imposent des nouveaux devoirs pour ces entreprises. Elle peut paraître paradoxale sachant que certains organismes gouvernementaux ont accès aux données personnelles de l'utilisateur ; néanmoins leur finalité est différente, le gouvernement cherche tout d'abord à repérer et empêcher tout acte de cybercriminalité et de terrorisme alors que les GAFAM cherchent à accéder à nos données à des fins purement commerciales.

Ce règlement européen a fait beaucoup de bruit, il y a eu une véritable prise de conscience des citoyens européens sur leurs droits et sur la protection de leurs données personnelles. Les GAFAM ont finalement dû se contraindre à renforcer la protection des données des citoyens et à plus de transparence pour éviter des sanctions économiques très sévères.

A moyen terme, il est souhaitable qu'un outil de type traité international prenne exemple sur le règlement européen afin d'harmoniser au niveau mondial cette protection des données personnelles mise en place.

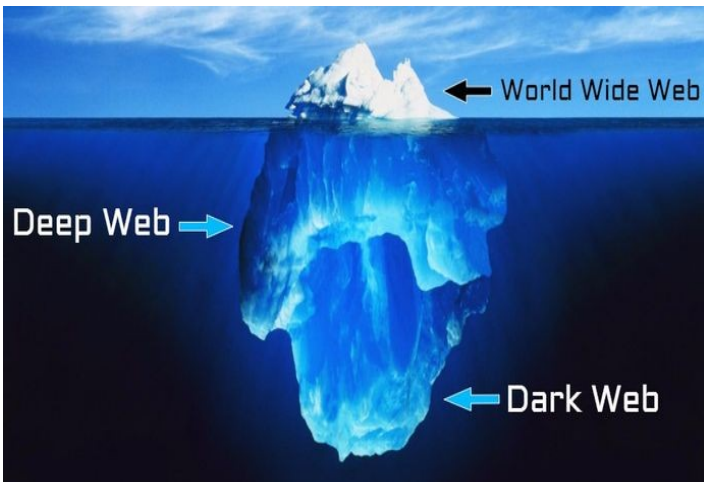
III. Le Darkweb

1. Deepweb, Darkweb et darknets

Si nous vous demandions quelles sont les différences entre le Darkweb, le Deepweb et le Darknet êtes-vous en mesure de nous répondre, ou pensez-vous que ces trois choses sont identiques ? Afin qu'il n'y ait pas de confusions sur ce qui va suivre nous allons expliquer la structure du web afin de mieux comprendre le Darkweb.

Nous allons tout d'abord commencer par définir ce qu'est le Web, ou World Wide Web[1]. Le web est donc un réseau d'information, utilisant internet comme support, composé des milliards de pages et autres documents liés entre eux via des liens hypertextes. Le web peut être ainsi comparé à une gigantesque toile d'araignée où les fils représenteraient les liens et les nœuds des documents. Nous avons accès à toutes ces données grâce à différents moteurs de recherches tels que Google. Ils parcourent les liens hypertextes avec des robots d'indexations afin d'analyser, suivant des critères qui leur sont propres, un maximum de contenu possible et savoir s'il est indexable ou non. Un contenu indexé pourra donc être accessible directement depuis le moteur de recherche en question. Toutes ces pages composent ce qu'on appelle le web visible et tout le reste, les documents auxquels on ne peut pas directement accéder depuis la barre de recherche, constitue le Deepweb.

Si des pages ne sont pas indexées, cela ne signifie pas qu'elles sont illégales ou dangereuses. En effet, il existe de nombreuses raisons pour lesquelles une page ne passe pas l'analyse des robots, ils peuvent tout simplement ne pas y avoir accès, c'est ce qu'on appelle des pages sans backlinks, c'est-à-dire qu'il n'y a pas de liens hypertextes pour les lier. C'est le cas par exemple lorsque vous achetez un billet d'avion. Le contenu peut aussi être trop volumineux pour être indexé ou bien encore le créateur de la page a pu décider de garder l'URL secret, on peut alors seulement y accéder en tapant l'adresse exacte. Contrairement à ce qu'on entend habituellement le Deepweb n'est donc pas illégal et nous l'utilisons même plus régulièrement que ce que l'on pourrait penser.



Si le Deepweb et le web visible sont deux choses bien distinctes, on différencie moins bien le Darkweb et le Deepweb. Le premier est une partie du second, où les usagers gardent l'anonymat. Le Darkweb est constitué de sous-réseaux, les darknets ils ne sont pas liés entre eux, à l'inverse des autres réseaux du web. Ils comportent aussi des protocoles d'anonymisation de de cryptage de l'adresse IP[2]. Les darknets utilisent donc un système qui ne partage pas publiquement vos données et utilise un chemin aléatoire empêchant toute traçabilité.

1 World Wide Web : abrégé en www, il est connu de tous pour faire parti des liens URL des pages d'internet.
2 Sans entrer dans les détails, l'adresse IP est une signature informatique de l'ordinateur renseignant les recherches internet de l'utilisateur.

2. Darkweb, le côté sombre du web ?

On nous dépeint souvent le Darkweb comme une partie sombre, mais est-il réellement dangereux ? Si l'internaute navigue sur le Darkweb, il ne risque pas grand-chose, sauf cas exceptionnels (ce qui peut aussi arriver sur le web visible). Il faut simplement toujours réfléchir à un élément clé : l'anonymat. En effet c'est la clé de voûte du Darkweb, ce qui signifie que dès le moment où l'utilisateur interfère avec une tierce personne il ne pourra pas le localiser. Si celle-ci est mal intentionnée elle peut nuire à l'utilisateur ; c'est notamment le cas s'il fait des échanges, il ne pourra jamais être sûr que l'interlocuteur remplira sa part du marché.

Si ce n'est pas si dangereux, pourquoi le Darkweb est vu comme la bête noire d'internet ? D'une part les entreprises telles que Facebook ou Google, utilisant les données personnelles de leurs utilisateurs, n'ont aucun intérêt à une navigation anonyme et contribue à dégrader l'image du Darkweb. D'autre part, il est vrai que le Darkweb héberge beaucoup de contenu illicite. On peut y trouver de nombreux marchés noirs d'armes, de drogues ou de faux papiers, mais aussi de la pédopornographie !

3. Le Darkweb au service de la liberté ?

Comme beaucoup d'inventions lorsqu'elles sont mises entre les mains de mauvaises personnes, le Darkweb a été détourné à des fins malsaines. Cependant le Darkweb permet aussi à des personnes bienveillantes de s'exprimer et d'en tirer des bénéfices. L'anonymisation de la navigation n'a pas attiré que des receleurs de produits illicites car de nombreuses personnes et organisations utilisent ce moyen pour diffuser leurs idées censurées sur le Web. Tout d'abord nous pouvons prendre l'exemple des hackers, même si certains d'entre eux cherchent simplement à disséminer des ransomware[1] pour faire du profit, nombreux sont ceux qui utilisent leurs savoir-faire à des fins plus justes. En effet, même si les hackers doivent flirter avec la légalité dans leurs agissements afin de prendre le contrôle d'un site ou d'un logiciel, lorsqu'il s'agit de mettre en avant la faiblesse du système de cyber défense, il est difficile de ne pas saluer ces actes. Ce fut notamment le cas en 1984, année durant laquelle l'organisme Chaos Computer Club a dérobé puis rendu plus de 100 000 deutsche mark à une banque allemande afin de mettre en évidence une faille. Quant à aujourd'hui de nombreuses organisations telles qu'Anonymous utilise le Darkweb pour mener des actions de grande ampleur. L'un de ces agissements est le nettoyage des sites pédopornographiques polluant les réseaux anonymes ; ceci est réalisé en faisant crasher les sites grâce à une attaque DDoS[2]. Enfin le Darkweb est aussi une zone de refuge pour les lanceurs d'alerte qui peuvent relayer leurs informations sans prendre de risques.

Le Darkweb est donc un moyen d'échapper à la surveillance de masse mais ne remplace pas un moteur de recherche classique, et bien que de nombreuses personnes l'utilisent pour le bien de la liberté d'expression, l'utilisateur doit se méfier quant aux intentions de ces actes.

1 Un ransomware est un logiciel néfaste pouvant bloquer une machine ou crypter des données personnelles, dont le seul moyen pour s'en débarrasser est de payer une rançon définie par le propriétaire du virus.

2 Une attaque DDoS ou déni de service est une cyber attaque visant à rendre indisponible un site en envoyant simultanément un nombre suffisant de requête pour le faire crasher.

IV. Dépendance

Dès notre enfance, nous avons pu être touchés par le multimédia, par diverses choses telles que les consoles vidéo, les ordinateurs et même les téléphones. Cela commence de plus en plus jeune au fil du temps avec la modernisation. Certaines personnes sont scotchées à leurs téléphones portables et ne peuvent s'en détacher sans se sentir mal.

Tout d'abord définissons le terme drogue. Le mot "drogue" désigne toute substance, naturelle ou synthétique, qui a un effet modificateur sur l'état de conscience et/ou l'activité mentale. C'est donc quelque chose dont nous sommes dépendants et dont nous ne pouvons pas nous passer sans que cela nous amène à un manque de quelque chose. Lors d'une utilisation intensive du téléphone portable, le cerveau sécrète de la dopamine, l'hormone du bonheur.

Nous pouvons parler d'une addiction quand par exemple nous nous servons du téléphone même lorsque nous sommes entourés de personne. Si quelqu'un travaille tous les jours sur ordinateur nous parlerons d'addiction à partir du moment où il continue de passer le reste de son temps sur un écran c'est-à-dire hors du travail. Steve Jobs, le créateur d'Apple, assurait ne pas avoir de tablette chez lui pour ses enfants car le travail et la vie réelle doivent bien être dissociés.

La première fois qu'a été nommée l'addiction à internet fut en 1995 par le docteur Ivan Goldberg qui pour « plaisanter » a cherché à appliquer les critères de trouble de dépendance à internet. Son article fut posté en ligne sur le site internet *PsyCom.net*. Néanmoins, dès 1996 la psychologue américaine K. Young présente les nouveaux critères définissant l'addiction à internet, ceux-ci étant calqués sur ceux des jeux. En effet, les troubles de dépendances à internet sont liés à un désordre de contrôle des pulsions tout comme pour les jeux pathologiques (jeux de hasard, jeux d'argent…). Ces critères sont sous forme de huit questions (traduction libre prise sur *psycho-ressources.com*):

- 1. Vous sentez-vous préoccupé par Internet (en pensant à votre dernière activité sur le Net et en anticipant votre prochaine session) ?
- 2. Éprouvez-vous le besoin de naviguer sur le Net pendant des périodes de plus en plus longues avant d'être rassasié ?
- 3. Avez-vous tenté à plusieurs reprises et sans succès de limiter, contrôler ou arrêter votre utilisation de l'Internet ?
- 4. Vous sentez-vous fatigué, épuisé, déprimé ou irritable lorsque vous tentez de limiter ou arrêter votre utilisation de l'Internet ?
- 5. Restez-vous sur le Net plus longtemps que ce que vous aviez prévu au départ ?
- 6. Avez-vous mis en danger ou risquez-vous de perdre une relation significative, un travail, une opportunité de carrière ou d'affaire à cause de l'utilisation d'Internet ?
- 7. Avez-vous menti à votre famille, votre thérapeute ou d'autres personnes afin d'avoir plus de temps pour utiliser l'Internet ?
- 8. Utilisez-vous Internet pour vous évader et échapper à vos problèmes ou à des émotions négatives (abandon, culpabilité, anxiété, déprime) ?

Le diagnostic est ici positif si le patient répond à plus de cinq questions par oui, néanmoins si déjà trois questions sont positives alors le patient sera un cas à haut risque.

De nos jours nous pouvons aussi rajouter comme signes qui montrent ce trouble : ne pas pouvoir sortir sans son téléphone, avoir le besoin de regarder toutes les cinq minutes si on a

reçu une notification, ne pas supporter de se retrouver sans réseaux (alors qu'on n'a pas besoin du téléphone), avoir besoin de regarder ses mails et messages en continues…

Cette pathologie est plus ou moins reconnue en fonction des pays, par exemple dès 2007 en Corée du Sud, de nombreuses structures sont mises en place afin de résoudre les problèmes d'addiction chez les jeunes : 140 centres de consultation, des programmes spéciaux dans une centaine d'hôpitaux et des « camps » inspirés des camps militaires. Dans les pays asiatiques, cette dépendance est traitée comme une vraie maladie. Pourtant dans les pays européens, seul des programmes de suivies thérapeutiques existent mais ceux-ci ne sont pas mis en avant. En France, l'Etat essaie de faire des campagnes préventives avec plusieurs affiches publicitaires.

Cette non-reconnaissance est due par la non identification de ce trouble dans le DSM-5. Le DSM-5 est la dernière édition (février 2018) *du manuel diagnostique et statistiques des troubles mentaux* de l'association de psychiatrie américaine.

Cette addiction est néfaste, le problème est de ne plus faire la différence entre virtualité et réalité et ceux sous tous les points : que ça soit au niveau des réseaux sociaux avec Facebook, Instagram ou même Twitter ainsi que du côté des jeux vidéo notamment ceux de combat et de violence. Il existe différentes manières de classifier la dépendance à internet :

D'après Young il y aurait 5 sous-types d'addiction :

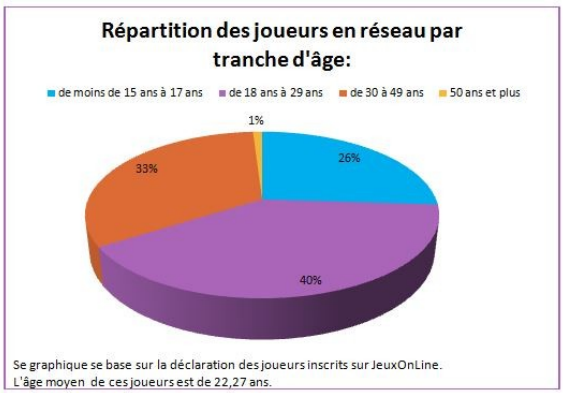
- L'addiction à la cyber sexualité
- L'addiction aux cybers relations
- Les compulsions sur internet
- La recherche compulsive sur internet
- L'addiction aux jeux vidéo en ligne

D'après Davis il y aurait seulement deux classes d'addiction :

- L'usage spécifique d'internet
- L'usage généralisé d'internet

Ces deux classements se rejoignent toutefois, la psychologue Young étant plus précise dans ce que Davis appelle « généraliser ».

En moyenne en Europe une personne âgée entre 15 et 19 ans passera trois heures sur son téléphone, contre deux heures pour une personne de 20 à 29 ans. Nous avons réalisé un sondage (confer partie V) dans deux écoles primaires afin de pouvoir analyser ce comportement face aux plus jeunes une classe de CM1 et deux classes de CM2). Nous pouvons voir que la plupart, 66%, ont déjà un téléphone portable ainsi qu'une tablette à disposition.



Certains parents n'imposent pas non plus de contraintes d'horaire, 53%. Néanmoins ceci peut mener à une addiction, donner des horaires limites peut permettre à l'enfant de comprendre qu'internet n'est pas une plateforme où nous pouvons passer tout notre temps. De plus quatre élèves de 10 ans étaient déjà actifs sur YouTube en tant que « youtubers » de jeux vidéo tel que Fortnite, et un des enfants n'avait pas prévenu ses parents de cette activité. On remarque bien ici le besoin de devoir être sur internet, quitte à ne pas prévenir afin qu'on ne puisse pas l'arrêter. D'après un autre sondage fait sur le site *JeuxOnline.com* on peut voir que presque 30% des joueurs réguliers sont âgés de moins de 17 ans.

Cependant de plus en plus de personne ressentent le besoin de se déconnecter, pour cela des voyages sans réseau existent. Les « digital detox » sont des voyages de 3 à 8 jours où les personnes partent généralement en groupe dans des endroits plus reculés afin de passer du temps entre eux et sans écran. Sur internet, de nombreux voyages de ce type sont proposés. Par exemple aujourd'hui des agences comme *Asia.fr* ou *Intothetribe.com* se sont créées dès 2015 en France et sont devenues de vrais business. Le concept plaît et conquis surtout les personnes très occupées par leur travail, elles peuvent ainsi reprendre contact avec elles-mêmes. Parmi les commentaires recensés sur le site *Intothetribe.com*, l'un des voyageurs nous parle de sa « grosse prise de conscience de l'hyperconnexion », de son bien-être après cette pause sans outil numérique, et de son envie de recommencer aussitôt le téléphone rallumé.

Mais selon une étude de l'académie des sciences, les écrans ont aussi de nombreux effets bénéfiques. En effet les écrans sont déconseillés avant les trois ans mais ils pourraient aider, plus tard, lors de l'apprentissage et de la motricité sensorielle. Entre trois et dix ans, les parents doivent contrôler l'utilisation des écrans, et apprendre aux enfants à s'auto-réguler, c'est-à-dire savoir quand s'arrêter. A l'adolescence, jouer aux jeux vidéo peut permettre de penser plus rapidement, logiquement et de réaliser plusieurs tâches à la fois. Les joueurs de jeux vidéo seront aussi plus attentifs et plus vifs.

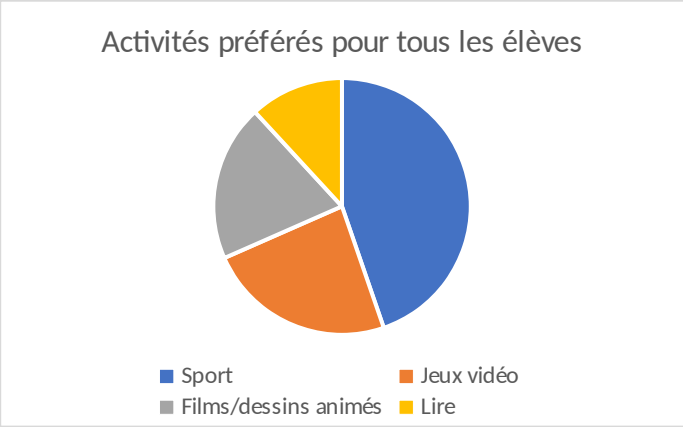
Pour conclure, les écrans, s'ils sont bien utilisés ne représente pas un risque en soi. On remarque toutefois une forte dépendance à internet mais celle-ci reste non-reconnue par les gouvernements. Néanmoins certains pays essaient tout de même de mettre en place des dispositifs afin d'aider les personnes atteintes de ce trouble comme le Portugal, la Grèce…

V. Sondage

Afin de mieux nous représenter l'addiction aux technologies numériques des enfants, nous avons réalisé un sondage auprès des élèves de CM1 et CM2. Ainsi, nous nous sommes rendus à l'école de Malintrat et à l'école du Masage à Beaumont. Nous avons en amont du sondage rencontré plusieurs fois le directeur de la dernière école afin de discuter des différentes questions à poser aux enfants, de la tournure des phrases, de la mise en forme… Ces rencontres nous ont été bénéfiques car elles nous ont permis de nous rendre compte de choses simples auxquelles nous n'avions pas pensé auparavant. En effet, il faut réussir à se mettre à la place des enfants de 10 ans, nous avons donc beaucoup discuter sur la mise en forme du sondage. Nous en avons déduit qu'il fallait éviter les mots trop compliqués, privilégier les QCM…

Une fois le sondage aboutit (confer Annexe), nous sommes allés dans les classes afin de guider les élèves, de répondre à leurs éventuelles interrogations et surtout échanger avec eux. Nous avions quatre questions majeures à leur poser. La première portait sur leurs activités préférées, en incluant des activités physiques, intellectuelles et numériques, afin de nous rendre compte de la prépondérance du numérique. Ensuite nous leur avons demandé de faire un classement entre différentes technologies dans l'objectif de voir lesquelles étaient les plus à même de créer une dépendance chez les enfants. Enfin pour connaître la proportion d'entre eux à avoir accès aux nouvelles technologies nous leur avons demandé s'ils possédaient ou non un téléphone et une tablette et s'ils l'avaient depuis plus d'un an ou non. Nous avions aussi posé quelques questions ouvertes sur l'utilisation et de la fréquence de ces technologies et s'ils pensaient pouvoir se passer d'internet.

La première question portait sur les activités préférées entre le sport, les jeux vidéo, la lecture, regarder des films/dessins animés. Nous avions donné la possibilité aux enfants de rajouter une activité même si elle n'était pas parmi les quatre (aucun d'eux ne l'a fait cependant) et d'en choisir une ou deux.



On remarque tout de suite que le sport représente à chaque fois une part importante quelle que soit la classe et le sexe de l'enfant et cela se retrouve sur le graphique global. On peut noter que les garçons aiment bien aussi les jeux vidéo et regardent peu de films ou dessins animés alors que chez les filles c'est plutôt le phénomène inverse. Le dernier graphique nous montre que les jeux vidéo sont quand même préférés aux films et à la lecture (qui eux sont équivalents). Nous nous attendions à ce que les garçons soient plus sportifs que les filles mais lisent beaucoup moins alors que ce n'est pas vraiment pas le cas. Nous pouvons en déduire que les activités physiques sont préférées aux activités numériques, cependant les enfants préfèrent jouer aux jeux vidéo ou regarder des films plutôt que de lire.

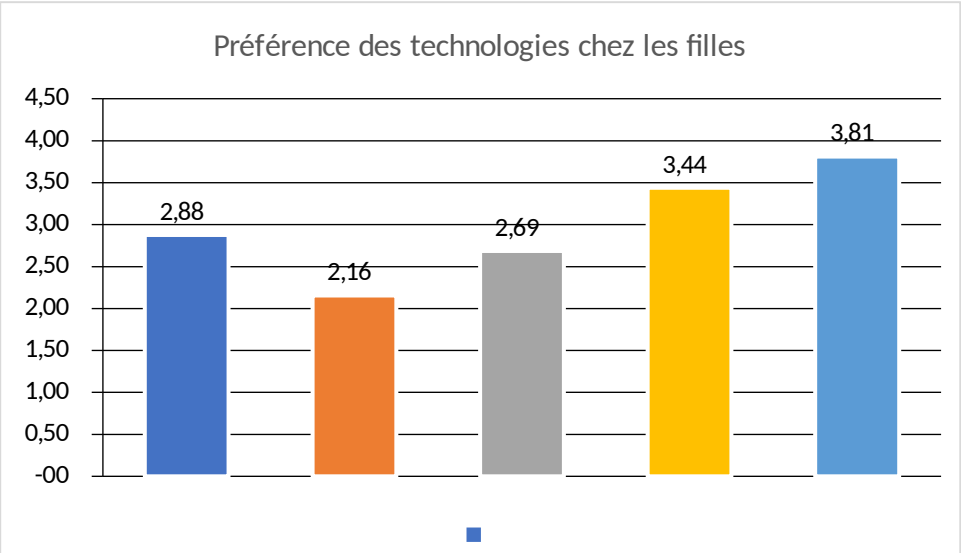
Les résultats de la question n°2 sont sans doute les plus compliqués à comprendre, des explications s'imposent donc. Nous avons demandé aux enfants de classer par ordre de préférence 5 technologies à savoir le smartphone, la télévision, l'ordinateur, la console et la tablette. Nous avons donc attribué à chaque technologie un nombre de points en fonction de sa place dans le classement (1 point pour la 1ere place, 2 points pour la 2e place … 5 points pour la dernière). Cela signifie que plus le « score » de la technologie est élevé, moins elle est aimée. Nous avons ensuite divisé ce score par le nombre de participants pour mieux pouvoir comparer les deux résultats :

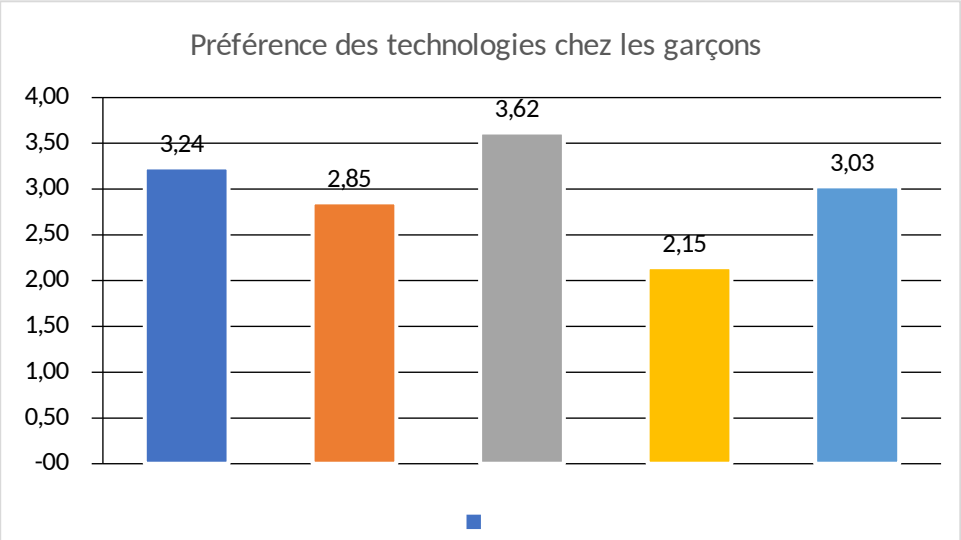
On obtient donc le classement suivant :

-Pour les filles : smartphone, télévision, tablette, console, ordinateur

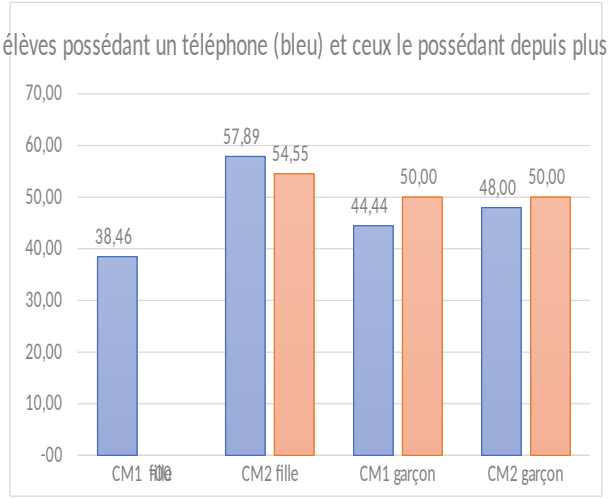
-Pour les garçons : console, smartphone, ordinateur, tablette, télévision

Nous pouvons remarquer que le smartphone est une technologie privilégiée par les filles mais aussi par les garçons, même s'ils préfèrent la console. Ensuite les résultats sont très hétérogènes et ne peuvent nous permettre de tirer aucune conclusion.





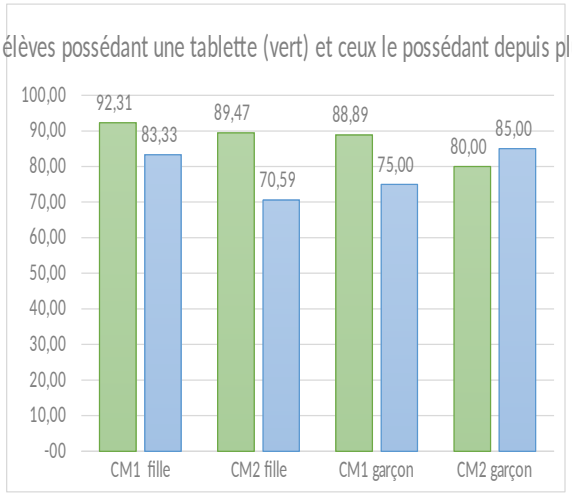
A travers la question suivante, nous avons cherché à savoir si les enfants possédaient un téléphone et s'ils l'avaient depuis plus ou moins d'un an :



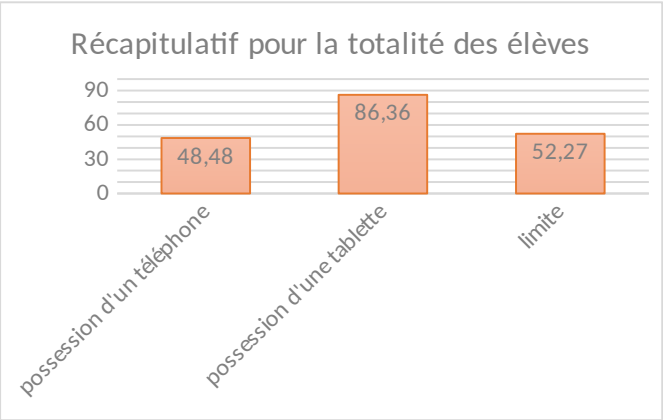
Sur ces données on voit que les résultats des garçons sont les mêmes quelle que soit leur classe, un peu moins de la moitié d'entre eux possèdent un portable et la moitié d'entre eux l'ont depuis plus d'un an. Les données des CM2 filles sont un peu plus élevé pour la possession du portable mais pas vraiment pour ce qui est de la durée. Pour ce qui est des filles en CM1 on remarque que les résultats sortent du lot, car aucune d'entre elles possède de téléphone depuis plus d'un an. Cela peut s'expliquer par le faible nombre de participants, il est donc plus probable d'avoir une anomalie.

Nous avons réitéré les deux mêmes questions pour la tablette, à la seule différence que pour le téléphone nous avions précisé aux enfants qu'ils devaient être à eux et non à leurs parents, alors que pour la tablette nous leur demandions juste s'ils avaient accès à une tablette (qu'elle soit à eux ou à leurs parents).

Comme pour les téléphones portables les résultats sont assez homogènes et le peu d'élèves sondés explique sûrement la différence entre ces chiffres, mais il ressort qu'une grande majorité des élèves ont accès à une tablette, et ce, depuis un moment.



Nous avons vu, la différence entre filles et garçons, CM1 et CM2, nous allons maintenant nous intéresser à trois données clé sur l'ensemble des élèves sondés sans différenciation :



Comme nous avions vu plus tôt, on voit que la moitié environ des enfants possèdent un portable alors que presque tous ont accès à une tablette. La dernière donnée porte sur une question secondaire où nous avions demandé aux enfants si leurs parents leur imposaient des restrictions horaires ou de durée sur l'utilisation des écrans. Nous voyons que seulement la moitié d'entre eux impose des limites à leurs enfants.

Enfin pour ce qui est des questions ouvertes nous n'avons pas fait de statistiques car les réponses étaient trop variées et l'échantillon trop faible. Nous en ressortons que les enfants utilisent leurs téléphones et les tablettes presque tous les jours, pour jouer à des jeux ou regarder des vidéos sur Youtube. La plupart d'entre avouent ne pas pouvoir se passer d'internet ou seulement pour quelques jours, lorsqu'ils partent en vacances par exemple.

Pour résumer, les enfants sont exposés très jeune aux nouvelles technologies. En effet, la moitié des élèves de 9 et 10 ans possède un smartphone et certains même depuis plus d'un an. De plus une très grande majorité d'entre eux a accès à une tablette, il en va donc de la responsabilité des parents de surveiller leurs enfants pour qu'ils ne deviennent pas dépendants. Cependant la moitié d'entre ne leur fixent même pas de limite.

VI. Google Home

1. Qu'est-ce que le Google Home ?

Google home est un haut-parleur intelligent qui réagit à nos demandes. Il est censé réagir après que quelqu'un dise « ok Google » ou « dis Google ». Grâce à ce système nous pouvons lancer un tas d'application ainsi que de la musique, faire des recherches etc. Google home a été créé par Google et met tous les appareils sous Google en commun. On peut donc dire « ok Google » à l'enceinte connectée et par exemple cela lance la musique du téléphone si les deux sont reliés. De plus c'est le même principe que nous avons sur nos téléphones, tablettes ou autres appareils connectés.

Néanmoins, si Google home réagis lorsque l'on dit « ok/dis Google » alors cela signifie peut-être que la technologie nous « écoute » en permanence. En effet il arrive que l'assistant de vie réagisse sans que l'on dise « ok Google » pourtant il lance quand même une recherche.

2. Sommes-nous en écoute permanente ?

Selon certaines recherches nous ne le sommes pas car cela serait visible depuis des opérateurs. De plus il n'est pas stipulé dans les conditions d'utilisation de Google que nous sommes écoutés. Depuis *myactivity.google.com* nous pouvons aussi savoir ce que nous avons fait, dit, regardé depuis notre compte Google et nous voyons que nos conversations habituelles ne sont pas enregistrées.

Mais nous savons par exemple qu'il retient nos déplacements ainsi que nos recherches, alors pourquoi pas ce que l'on dirait ? En recherchant sur l'historique, il y a des conversations qui ont été enregistrées qui n'ont pas de rapport avec Google, où il pense que l'on dit « ok Google ». Nous pouvons déjà en déduire que l'assistance de Google réagit peu importe ce qu'on dit tant que ça se rapproche de « ok/dis Google » donc que Google home est très sensible ce que nous disons afin de reconnaître les « ok/dis Google ».

3. Est-ce pour autant que Google enregistre ce que nous disons ?

D'après des expériences réalisées sur Youtube, nous savons aussi que lorsque nous parlons proche d'un appareil connecté à internet celui-ci peut nous proposer des publicités en rapport avec nos paroles. Par exemple nous parlons de vacances à un endroit x, et nos futures recherches contiendront des publicités pour des vols pour cet endroit susnommé. Nous pouvons expliquer ceci par l'acceptation des cookies sur nos moteurs de recherches et différents sites web utilisés. En effet en acceptant ces cookies, nous acceptons aussi leur écoute et par conséquent les publicités ciblées.

Maintenant que Google s'implante dans les foyers via le Google Home, nous nous sommes demandé si Google nous espionne à travers ces nouveaux assistants de vie. Si oui est ce que cela signifie que Google stocke des millions d'heures d'enregistrement dans le monde ?

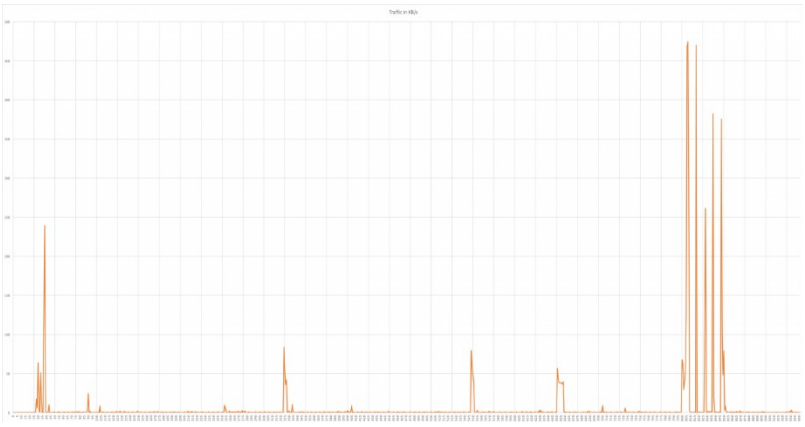
Pour répondre à cette question nous avons essayé « d'écouter » un Google Home pour savoir si des données sont envoyées même lorsqu'on ne lui demande rien ou qu'il est éteint. Nous allons pour cela nous servir de Wireshark. C'est un logiciel qui permet d'observer si des

données passent par notre box Wi-Fi en temps réels. Pour cela nous nous sommes munis d'un ordinateur sous Linux. Puis avec un câble Ethernet et une box Wi-Fi nous avons créé un hotspot[1] Wi-Fi sur cet ordinateur. On peut considérer que l'ordinateur est devenu une nouvelle box Wi-Fi, un point d'accès qui intercepterait à l'aide de Wireshark les données émises par le Google Home. Une fois connecté à cette « nouvelle box », nous pouvons lui poser des questions simples, essayé de l'interroger alors qu'il est éteint, que le micro est désactivé ou encore simplement parler à côté. Nous aurions ensuite observé en isolant l'enceinte connectée avec son adresse IP, quand des données étaient émises.

Cependant nous avons rencontré de nombreuses difficultés lors de la réalisation de cette expérience, notamment lors de la création du point d'accès sur l'ordinateur Linux. Finalement une fois le Hotspot créé, il s'est avéré que le Google Home ne parvenait pas à se connecter dessus ou bien qu'il n'émît aucune donnée.

La source du problème peut alors être multiple :
-Une connexion trop faible pour le Google Home.
-Une mauvaise clé Wi-Fi qui ne parvenait pas à émettre la Wi-Fi.
-Tout simplement le Google Home qui ne peut pas se connecter à un Hotspot Wi-Fi, en effet de nombreuse personne ne parvienne pas à connecter leur assistant personnel à un point d'accès Wi-Fi.

Nous sommes déçus de n'être pas parvenus à conclure cette expérience mais entre l'année dernière et cette année des personnes sont parvenues à observer les données émises par des Google Home notamment sur le site *labs.sogeti.com* et il s'avère qu'il n'y aurait rien de suspect à signaler. Lorsque le micro ou l'enceinte est éteinte il n'envoie aucune donnée et lorsqu'on lui pose une question il n'émet des données seulement quelques secondes soit le temps de répondre à la question posée. Nous avons été surpris de découvrir cela puisque nous avions peur de découvrir que les assistants personnels nous écoutent à chaque instant.



Les pics représentent les données envoyées par l'enceinte connectée. Les pics ne sont présents que pendant les cinq secondes où une question a été posée.
Cependant est ce que cela signifie que Google n'utilise pas ces nouveaux produits pour connaître nos habitudes ? Non, les Google Home stockent tout de même tout notre historique pour savoir de quoi est fait notre quotidien et enregistre chaque question mais il est tout de même rassurant de savoir qu'il ne nous écoute pas lorsqu'on ne le questionne pas.

En testant simplement, le téléphone verrouillé et écran éteint, Google ne s'active pas à l'entente de « ok/dis Google » mais si l'écran est allumé à ce moment-là alors l'assistant Google se met en marche.

1 Le hot spot est un point d'accès Wi-Fi, plus connu sous le nom de borne Wi-Fi.

Conclusion

A travers ce projet, la puissance des GAFAM dans le monde s'est révélé être en symbiose totale avec l'idéologie capitaliste. Elle est comparable à un pays tel que celui de l'Allemagne.

Les GAFAM ont réussi à se rendre indispensable dans notre quotidien même si nos actes peuvent être utilisés et revendus. Tout ce que nous faisons sur les réseaux est retenu et peut être utilisé à notre insu.

Les lanceurs d'alerte ont grandement contribué à éveiller notre esprit critique sur l'utilisation consenti de nos données personnelles et à avertir sur les différentes conséquences de nos actes sur internet. Les GAFAM peuvent, grâce à nos décisions sur le web, nous connaître mieux que n'importe qui.

Différentes méthodes pour nous espionner sont ressorties, par exemple les micros d'ordinateur ou de téléphone, ainsi que les flux de données. Néanmoins, le Google Home ne sert pas "d'oreille" directement dans nos maisons.

De plus de nombreuses lois sont maintenant en vigueur afin de nous protéger et de protéger les lanceurs d'alertes. Peut-être que grâce à elles, un jour nous pourrons être libres de nos faits et gestes. Nous avons aussi trouvé un moyen de rester dans l'anonymat, le Darkweb, qui nous protégerait de la revente de données.

Cependant nous pouvons nous demander si les GAFAM pourront continuer dans cette voie. En effet Google enchaîne les différentes amendes avec par exemple une de 50 millions d'euros datant du 21 janvier 2019. Ces puissances seront-elles toujours aptes à nous espionner dans quelques années ? Nous pourrions même nous demander, si elles ne pourraient pas devenir totalement indépendantes et passer aux dessus des lois régissant notre société actuelle.

Sitographie

https://www.generation-nt.com/nsa-localisation-smartphone-transmission-signal-actualite-1813262.html

https://www.psychologies.com/Moi/Problemes-psy/Dependances/Interviews/Les-reseaux-sociaux-peuvent-ils-devenir-une-veritable-addiction

http://boulevardduweb.com/addiction-reseaux-sociaux/

http://psychaanalyse.com/pdf/RECHERCHE%20D%20UNE%20ADDICTION%20AUX%20RESEAUX%20SOCIAUX%20ET%20ETUDE%20DU%20PROFIL%20D%20UTILISATEUR%20CONCERNE%20-%20THESE%20EN%20PSYCHIATRIE%202012%20(209%20Pages%20-%204,3%20Mo).pdf

https://fr.wikipedia.org/wiki/Manuel_diagnostique_et_statistique_des_troubles_mentaux

https://lacyberdependance2017.wordpress.com/2017/01/09/la-cyberdependance-chez-les-jeunes-adolescents/

https://www.liligo.fr/magazine-voyage/digital-detox-voyage-deconnecte-41032.html

http://www.psycho-ressources.com/bibli/cyberdependant.html

http://www.atlantico.fr/decryptage/accro-votre-telephone-portable-scientifiques-expliquent-pourquoi-gerard-yves-cathelin-2661319.html
http://leplus.nouvelobs.com/contribution/523776-pourquoi-devient-on-accro-a-son-telephone-portable.html

https://books.google.fr/books?hl=fr&lr=&id=ikBmDwAAQBAJ&oi=fnd&pg=PP1&dq=d%C3%A9pendance+aux+gafam&ots=Q0U0GqbkFR&sig=Srkjv73iaUEjhftgf8cp1w3_BGA#v=onepage&q&f=false
https://labs.sogeti.com/google-home-spying/?fbclid=IwAR3K3mx8WywosJZ7e3x5IMxlEldVkbIjGCCMHJMAfSogThV05pjQZz57S7s

https://www.youtube.com/watch?v=hLpAT5bu2uk&feature=youtu.be&fbclid=IwAR1HDN47TZIwIOLGypXrTmPa8-NhF0cfCt8pU7c0tbIaY9T6xxkXiM7hrhs

CNIL : https://www.cnil.fr/

www.youtube.com

https://wikileaks.org/

Annexes

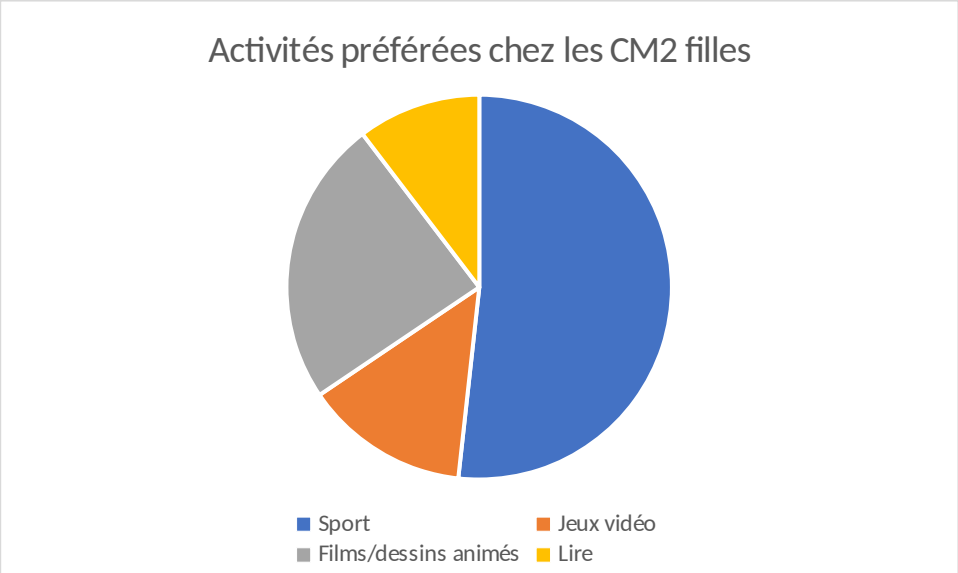


Figure 1 Activités CM2 filles

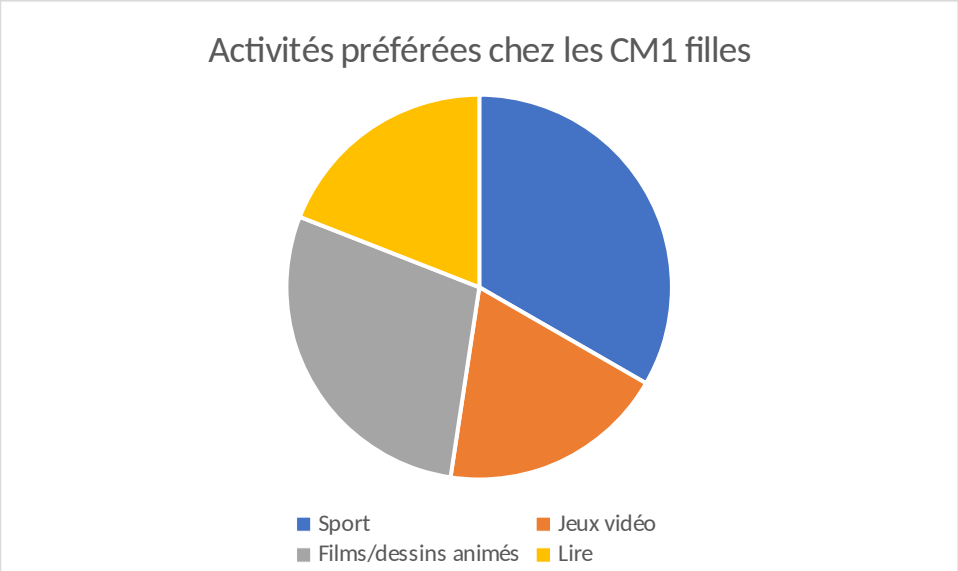


Figure 2 Activités CM1 filles

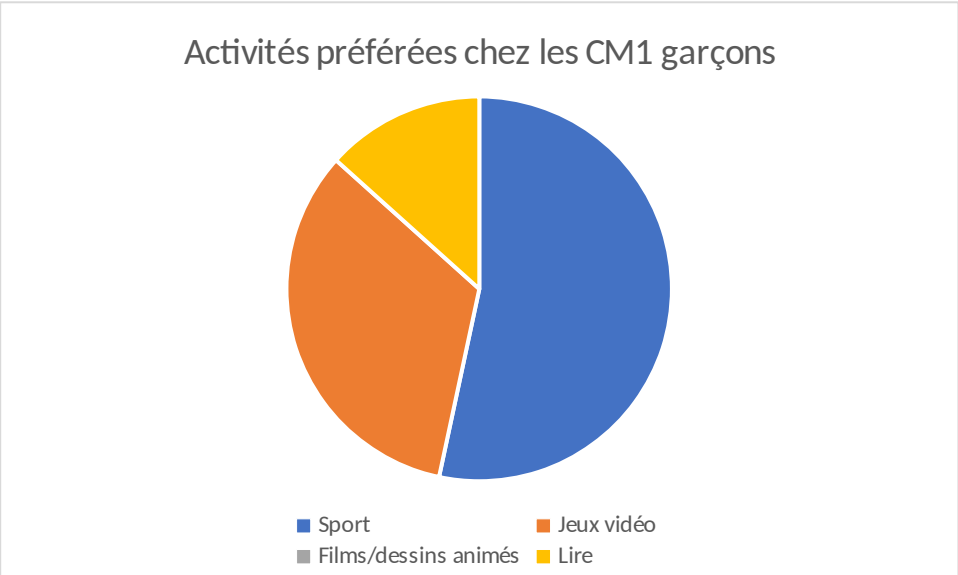


Figure 3 Activités CM2 garçons

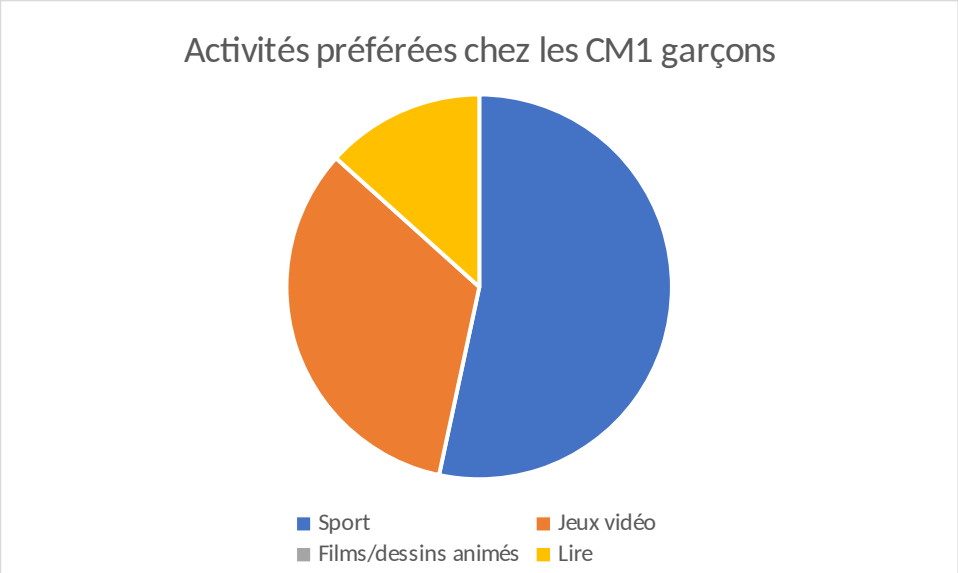


Figure 4 Activités CM1 garçons