h e g

Haute école de gestion
Genève

L’avenir du web réside-t-il dans sa décentralisation ?

Travail de Bachelor réalisé en vue de l’obtention du Bachelor HES

par :

Favre Alan

Conseiller au travail de Bachelor :

Mr. Ciaran Bryce

Genève, le 17.09.2021

Haute École de Gestion de Genève (HEG-GE)

Filière Informatique de Gestion

Hes·so GENÈVE
Haute Ecole Spécialisée
de Suisse occidentale

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre de Bachelor of Science HES-SO en informatique de gestion.

L'étudiant a envoyé ce document par email à l'adresse remise par son conseiller au travail de Bachelor pour analyse par le logiciel de détection de plagiat URKUND, selon la procédure détaillée à l'URL suivante : https://www.urkund.com .

L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Anières le 17.09.2021

Favre Alan

Remerciements

J’aimerai remercier Mr. Bryce qui a accepté de suivre ce travail durant les 8 semaines de rédaction. Son expertise ainsi que ses conseils ont été précieux durant la réalisation de ce travail de recherche.

Résumé

Le web que nous utilisons actuellement est trop centralisé. Le pouvoir sur le web appartient à quelques entreprises américaines ainsi qu'aux gouvernements de la planète qui nous surveillent et censurent le contenu qui ne leur plaît pas.

Cette centralisation pose un gros problème car elle va à l'encontre des valeurs sur lesquelles le web se repose, à savoir la démocratie ainsi que la liberté d'expression et de la presse.

Au-delà de ces valeurs qui ne sont aujourd'hui plus respectées, plusieurs autres problèmes sont causés par cette centralisation excessive. Ces problèmes concernent les points suivants :

- Les services mis à disposition par les entreprises
- Les données que nous fournissons aux entreprises
- Les conditions d'utilisation des services
- L'infrastructure qui supporte le web actuel
- Les capacités de contrôle et de censure des gouvernements

Dans ce travail, il sera question des solutions qu'il existe actuellement afin de bâtir un web décentralisé qui respecte les principes fondateurs de ce dernier.

Ces solutions seront explorées techniquement puis il sera ensuite question des avantages que propose un web décentralisé. Afin de faire écho aux problèmes du web centralisé, ces avantages seront analysés selon les mêmes axes, à savoir :

- Les services
- Les données
- L'infrastructure
- L'environnement
- Le pouvoir des gouvernements

Il sera également question des dérives d'un système décentralisé car celles-ci existent aussi. Ce chapitre se terminera par une analyse des actions de certains gouvernements afin de réduire le pouvoir des grandes entreprises américaines.

Enfin, nous nous rendrons compte via une marche à suivre qu'il n'est pas difficile pour tout un chacun de participer à ces projets de web décentralisés afin d'assurer un futur numérique libre aux générations futures.

Table des matières

Liste des figures

1. Introduction

Le web est un outil formidable que nous utilisons tous de manière quotidienne. Difficile aujourd'hui d'imaginer un monde sans le web riche que nous parcourons durant des heures, surtout dans les conditions de vie difficile de ces derniers mois.

En effet, encore plus qu'en temps normal, cette pandémie mondiale a permis de se rendre compte que le web est un outil formidable pour rester en contact avec ses proches, travailler depuis la maison ou encore se divertir lorsqu'on en a besoin.

Pour la plupart des gens, l'utilisation du web ne pose aucun problème et représente une expérience agréable grâce aux services bien pensés des grandes entreprises, principalement américaines.

Mais en coulisses, le web est en train de mourir justement à cause de ces grandes entreprises. Le web, qui se voulait à la base comme un gigantesque réseau de réseaux ou n'importe qui peut apporter sa pierre à l'édifice, est aujourd'hui un empire contrôlé par quelques entreprises.

Leur pouvoir est tellement grand qu'il est estimé supérieur au pouvoir de certains pays sur la planète[1]. S'ils le veulent, ces géants peuvent du jour au lendemain mettre le monde à genou en arrêtant leurs services qui sont utilisés par des milliards de personnes.

Aujourd'hui, le web est trop centralisé. Le pouvoir est trop concentré et cela pose un grand nombre de problèmes qui vont être abordés dans ce travail.

Afin d'apporter des solutions à cette centralisation problématique, un certain nombre de projets existent. Ces projets cherchent à remettre le web entre les mains du peuple.

Ces projets seront abordés dans ce travail afin de comprendre comment un web non centralisé est possible et réalisable. Il sera également abordé la participation de chacun à ces projets afin de se rendre compte qu'il n'est pas difficile de faire partie d'une communauté qui souhaite retrouver sa liberté sur un web libre.

[1] https://teahouse.fifty-five.com/en/glossary/gafa/

2. La situation actuelle

En moins de 30 ans depuis sa création initiale au début des années 1990, le web a révolutionné le monde. Aujourd'hui, peu importe le domaine d'activité, les processus sont impactés d'une façon ou d'une autre par une intervention du web.

C'est également devenu un outil indispensable de nos vies privées. Que cela soit pour se divertir, s'informer ou encore rester en contact avec nos proches, nous utilisons tous le web de manière quotidienne.

Ce qu'on appelle le web est en fait un service qui s'appuie sur l'infrastructure d'Internet. On confond souvent les deux termes mais il est important de bien faire la différence. Internet représente l'infrastructure mondiale qui permet d'interconnecter les différents serveurs. Cette infrastructure englobe les centres de données, tous les appareils disposant d'un accès à Internet ou encore les câbles sous-marins qui relient les continents entre eux.

Le web quant à lui est un service qui permet, via Internet, de consulter des pages avec un navigateur en utilisant les adresses des sites.

Le problème actuel du web, c'est sa centralisation excessive. En effet, les quatre géants du web, communément appelés les GAFA (Google, Apple, Facebook et Amazon), accaparent tout et ne laissent que des miettes aux autres acteurs du secteur.

Dans ce premier chapitre, je vais expliquer pourquoi cette centralisation est un problème et quels sont ses impacts. Les problèmes sont multiples mais ils vont être abordés selon plusieurs thématiques : les services, les données, les conditions d'utilisation, l'infrastructure et pour terminer, la surveillance et censure des gouvernements.

Afin de comprendre comment et pourquoi le web est actuellement si centralisé, je vais également passer en revue les différents points historiques qui nous ont menés là où nous en sommes aujourd'hui.

2.1 Historique

L'idée d'interconnecter des ordinateurs afin d'échanger des informations remonte à environ 30 ans avant l'invention du web tel qu'on l'utilise aujourd'hui. Déjà en 1960, un professeur du MIT, J.C.R. Licklider, décrit pour la première fois les interactions qu'il est possible de mettre en place entre plusieurs ordinateurs afin de former un réseau.

C'est en 1966 que le premier réseau réel d'ordinateurs voit le jour, il s'agit d'ARPANET. Ce réseau a permis de prouver que la communication par paquets de données fonctionne et il a posé les bases du fonctionnement de tous les transferts de données que nous réalisons toujours aujourd'hui.

Les années qui suivent voient la création de nombreux protocoles de communication qui sont toujours utilisés de nos jours, notamment TCP/IP qui a été inventé par Robert E. Kahn en 1972. Il fut obligé d'inventer un nouveau protocole car celui utilisé jusqu'alors sur ARPANET, le protocole NCP, ne permettait pas de communiquer avec des hôtes en dehors du réseau ARPANET et ne gérait pas les éventuelles erreurs de transmission.

Plusieurs réseaux voient le jour au fur et à mesure des années et la plupart d'entre eux s'interconnectent afin de pouvoir échanger des informations. Dans les années 1980, c'est notamment le cas du CERN, le centre européen de recherche nucléaire, basé à Genève, et de l'ARPA, une agence gouvernementale américaine chargée des nouvelles technologies à usage militaire.

C'est en 1990 que le HTML est inventé par deux chercheurs du CERN, Tim Berners-Lee et Robert Cailliau. Le langage HTML, basé sur l'usage de balises, permet de créer des pages contenant du texte et des images ainsi que des liens qui vont rediriger vers d'autres pages.

Ces pages sont adressables via leur URL, ce qui représente leur adresse d'un point de vue des serveurs. Afin de transmettre le contenu des pages d'un serveur vers son client, c'est le protocole HTTP qui est utilisé. C'est la naissance du web tel qu'on le connaît et utilise aujourd'hui.

L'avantage du web, c'est que les différentes pages et les différents sites web n'ont pas besoin de s'organiser entre eux. En effet, n'importe quelle page peut contenir un lien vers une page d'un autre site sans que cela ne pose aucun problème. Cela fonctionnera évidemment seulement si le lien existe toujours.

Ces liens justement, comment le web fait-il pour savoir que wikipedia.org, qui est un nom de domaine, correspond au serveur avec l'adresse IP 91.198.174.192 par exemple ?

Comme je l'ai expliqué précédemment, le terme Internet fait référence à tous les réseaux disponibles qui sont interconnectés entre eux. Ces réseaux savent où envoyer les paquets qu'ils reçoivent justement grâce à l'adresse IP que ces derniers contiennent comme destination. Alors comment passer d'une requête pour wikipedia.org à l'adresse IP du serveur en question ?

Cette procédure est prise en charge par les serveurs DNS. Le but de ces serveurs, c'est de traduire en adresse IP le nom de domaine qu'il reçoit. Pour que cela fonctionne, il faut que ces serveurs DNS connaissent un maximum de noms de domaines et leurs équivalents en adresses IP. C'est donc la seule partie du web qui se doit d'être centralisée afin qu'en s'adressant à n'importe quel serveur DNS, l'adresse IP équivalente soit récupérée.

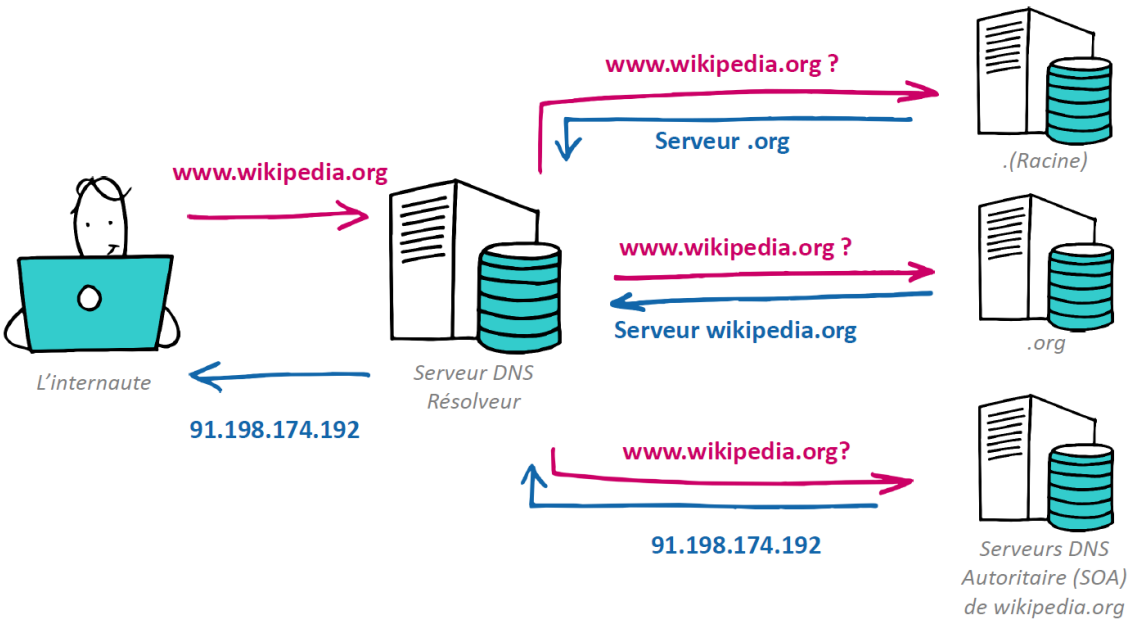

Figure 1 : Illustration d'un utilisateur souhaitant accéder à wikipedia.org
Source : https://www.nameshield.com/ressources/lexique/dns-domain-name-system/

De nos jours, chaque fournisseur d'accès à Internet exploite ses propres serveurs DNS afin de réduire le temps de latence de ses clients. Le fait d'utiliser un serveur DNS appartenant à l'entreprise permet également aux fournisseurs d'accès d'établir quelques règles, comme par exemple le fait de ne pas fournir l'adresse IP de certains serveurs que l'entreprise ou alors le gouvernement du pays en question estiment comme dangereux.

Il existe toutefois des registres DNS public que certaines entreprises du web mettent à disposition. On peut citer par exemple le serveur DNS de Google, celui d'OpenDNS qui appartient à Cisco ou encore le DNS de CloudFlare, entreprise bien connue qui permet de protéger son site derrière une infrastructure solide qui permet de réduire l'impact d'éventuelles attaques.

L'utilisateur peut modifier à son gré le serveur DNS qu'il utilise afin par exemple d'accéder à des sites que le pays dans lequel il se trouve a fait bloquer par les fournisseurs d'accès.

Mise à part ces serveurs DNS, le web devait être un environnement complètement décentralisé. Chaque personne possédant un appareil capable d'héberger un serveur web pouvait mettre à disposition du monde entier son site web.

Cette facilité d'accès et d'exploitation a permis au web de se développer de manière extrêmement rapide. En 2000, il existait environ 17 millions de noms de domaines uniques. Aujourd'hui, il existe 95 fois plus de noms de domaines uniques soit 1,7 milliard[2].

Aujourd'hui, la quantité d'information présente sur le web est colossale. Selon une estimation réalisée par le site physics.org, un téléchargement complet des 6 milliards de pages que contient le web avec une connexion classique de 44 Mbits/s nécessiterait plus de 3 millions d'années de téléchargement.

Cette décentralisation et la facilité de mise en place d'un site web ont certes permis au web de se développer rapidement mais cela a aussi créé des problèmes. En effet, à moins de connaître l'adresse du site que l'on souhaite consulter, il est impossible de le trouver.

[2] https://websitesetup.org/news/how-many-websites-are-there/

C’est dans cette brèche que se sont glissés les moteurs de recherche, dont le plus connu est sans équivoque Google. Sans un moteur de recherche performant capable de trouver les pages qui correspondent à un critère de recherche, il est impossible d’utiliser le web de manière intelligente car il est tout simplement impossible de trouver l’information par ses propres moyens.

La seconde faiblesse de cette décentralisation, ce sont les liens cassés. Un lien cassé est un lien dont la ressource pointée n’existe plus ou a été déplacée. Dans la majorité des cas, lorsqu’on clique sur un lien cassé, une erreur 404 va être affichée. Cette erreur signifie à l’utilisateur que la ressource qu’il cherche à atteindre n’existe pas.

2.2 Le pouvoir des géants du web

Revenons maintenant à nos géants du web, les GAFA. Comment ont-ils fait pour accumuler autant de puissance et pourquoi cela pose t'il problème ? Dans la suite de ce chapitre, je vais m'intéresser aux différents produits que ces entreprises proposent et je vais exposer des statistiques afin de démontrer l'emprise extrême qu'elles exercent sur le secteur.

2.2.1 Les services

La popularité et la puissance de ces géants du web est principalement générée grâce aux nombreux services que ces entreprises proposent à tout un chacun. Nous allons rapidement nous rendre compte qu'il y a peu de concurrence entre ces géants du web.

En effet, ils ont tous leur zone d'expertise dans laquelle ils excellent et ils ne s'occupent pas des domaines où ils savent qu'il leur sera très difficile de se faire une place. Il existe toutefois quelques exceptions ou ces géants se font concurrence.

2.2.1.1 Google

La première lettre de l'acronyme GAFA, le G, correspond au géant Google. Créée en 1998 par Larry Page et Sergey Brin et basée en Californie, l'entreprise est le leader incontesté de la recherche sur le web. Grâce à leur puissance surdimensionnée et à leurs algorithmes très performants, leur indexation du web est la plus performante et la plus complète.

En Avril 2019, 88.47% des recherches effectuées via un moteur de recherche ont été demandées à Google[3]. Cette part de marché est absolument gigantesque et représente bien la mainmise de Google sur ce domaine. Les 11.53% restants sont partagés entre Yahoo, Bing et Baidu.

En 2004, Google lance Gmail, une plateforme permettant à ses utilisateurs de recevoir et d'envoyer des emails, moyennant bien sûr la création d'un compte Google. Ce service remporte également un succès fou grâce à sa facilité d'utilisation et ses nombreuses fonctionnalités.

En 2021, sur les 4.03 milliards d'adresses emails enregistrées, 1.8 milliard sont des adresses Gmail[4]. Cela représente quasiment la moitié des adresses totales ce qui fait de Gmail le service avec le plus d'utilisateurs au monde.

[3] https://fr.statista.com/statistiques/559394/part-de-marche-mondiale-des-moteurs-de-recherche-2010/
[4] https://techjury.net/blog/gmail-statistics/

Fin 2006, Google achète pour 1,65 milliard de dollars une jeune plateforme de partage de vidéos créée une année auparavant, YouTube. Depuis cette acquisition, Google n'a cessé de faire évoluer la plateforme qui est aujourd'hui le leader incontesté du partage de vidéos sur le web.

En effet, YouTube compte 2 milliards d'utilisateurs actifs chaque mois[5], ce qui représente un quart de la population mondiale. Le chiffre concernant la quantité de vidéos publiées sur YouTube donne le tournis car environ 500 heures de vidéos sont publiées chaque minute sur la plateforme[6].

Toutefois, le chiffre le plus impressionnant à propos de la plateforme de partage de vidéos de Google concerne la proportion du trafic mobile mondial que le site accapare. En effet, la plateforme représente à elle seule 37% de l'entièreté du trafic sur appareils mobiles[7].

Au fur et à mesure des années, l'entreprise qui a démarré avec un seul service, à savoir le moteur de recherche, s'est constamment étendue à d'autres domaines et possède aujourd'hui des dizaines de produits.

Au-delà de ceux déjà cités, on peut ajouter Google Drive, la solution de stockage de fichiers en ligne proposée par Google aux particuliers ainsi qu'aux entreprises. Couplée à Google Docs, qui permet de rédiger des documents, tableurs et présentations de manière collaborative, la plateforme est très complète et possède un grand nombre d'utilisateurs. Google Drive est le leader du stockage de fichiers en ligne avec pas moins de 35.76% de parts de marché. Les principaux compétiteurs, à savoir Dropbox et OneDrive (Microsoft), se partagent respectivement 20.65 et 13.66% des parts de marché restantes[8].

[5] https://backlinko.com/youtube-users
[6] https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/
[7] https://www.journaldugeek.com/2019/03/26/youtube-represente-37-trafic-internet-mobile/
[8] https://www.datanyze.com/market-share/file-sharing--198/google-drive-market-share

Enfin, on peut citer Google Maps, le service de cartographie en ligne proposé par Google. Le service est extrêmement utilisé à travers le monde et son usage représente plus de 60% des parts de marché du domaine[9]. On peut également ajouter la plateforme de traduction de Google ou encore le navigateur qu'ils mettent à disposition, Chrome, qui est sans équivoque le navigateur le plus utilisé actuellement avec une nouvelle fois une part de marché supérieure aux 60%[10].

Pour terminer, on se rend bien compte en parcourant les différents services proposés par Google que l'entreprise n'est plus simplement un moteur de recherche. C'est un réel empire qui, certes cherche à simplifier et améliorer notre quotidien, mais s'immisce tout de même partout sans que nous nous en rendions toujours compte. Les parts de marché astronomiques de la plupart de leurs services montrent bien que notre dépendance à Google est extrêmement forte et que le web ne serait plus le même sans eux.

[9] https://www.datanyze.com/market-share/mapping-and-gis--121/google-maps-api-market-share

[10] https://gs.statcounter.com/browser-market-share

2.2.1.2 Apple

La deuxième lettre de l'acronyme, le premier des deux A, correspond à l'entreprise américaine Apple. Le cas de cette entreprise est un peu spécial car contrairement aux trois autres étudiées ici, le principal domaine ne concerne pas directement le web.

En effet, l'entreprise dirigée à l'époque par le brillant Steve Jobs, est surtout connue et réputée pour avoir révolutionner le monde tel qu'on le connaît aujourd'hui. Difficile d'imaginer la société actuelle sans un smartphone constamment à notre portée et cette avancée, nous la devons en grande partie à Apple qui a lancé leur produit phare, l'iPhone, en juin 2007 sous une pluie d'applaudissements.

Ce qui fait le succès d'Apple aujourd'hui, c'est principalement leurs produits hardware qu'ils vendent dans leur plus de 500 magasins à travers le monde. Le but d'Apple est de créer un écosystème pour ses utilisateurs avec plusieurs appareils de la marque qui communiquent entre eux et doivent permettre d'améliorer la qualité de vie de l'utilisateur.

Malgré cela, depuis quelques années, Apple cherche également à se faire une place au niveau des services aux utilisateurs. Ces services, souvent uniquement accessible via un appareil de la marque, viennent concurrencer notamment la mainmise de Google sur certains secteurs.

On peut notamment citer Apple Plans qui est disponible sur tous les appareils à la pomme. Ce service de cartographie est en concurrence directe avec Google Maps mais peine à se faire une réelle place dans le secteur. Le service a été développé justement pour se passer des services de Google sur les appareils Apple mais un démarrage manqué a grandement réduit ses chances de devenir le leader du domaine.

Malgré une amélioration certaine ainsi que l'ajout de quelques fonctionnalités exclusives, l'application ne représente aujourd'hui que 25% des utilisations totales d'un service de cartographie sur un appareil mobile[11]. A titre de comparaison, l'utilisation de Google Maps est d'environ 50% sur les appareils mobiles.

[11] https://www.isucorp.ca/blog/the-best-navigation-app-apple-maps-vs-google-maps

On peut également citer le service email d'Apple qui a grappillé des parts de marché au fur et à mesure depuis sa création et qui aujourd'hui en possède plus que le rival Google. En effet, on se rend compte sur le graphique ci-dessous qu'Apple possède 40% des parts de marché en 2020 alors que Google les talonne avec 38%[12]. Les parts restantes sont partagées entre Outlook, propriété de Microsoft et Yahoo, grand acteur historique du web qui peine à se mettre au niveau de ses compétiteurs.

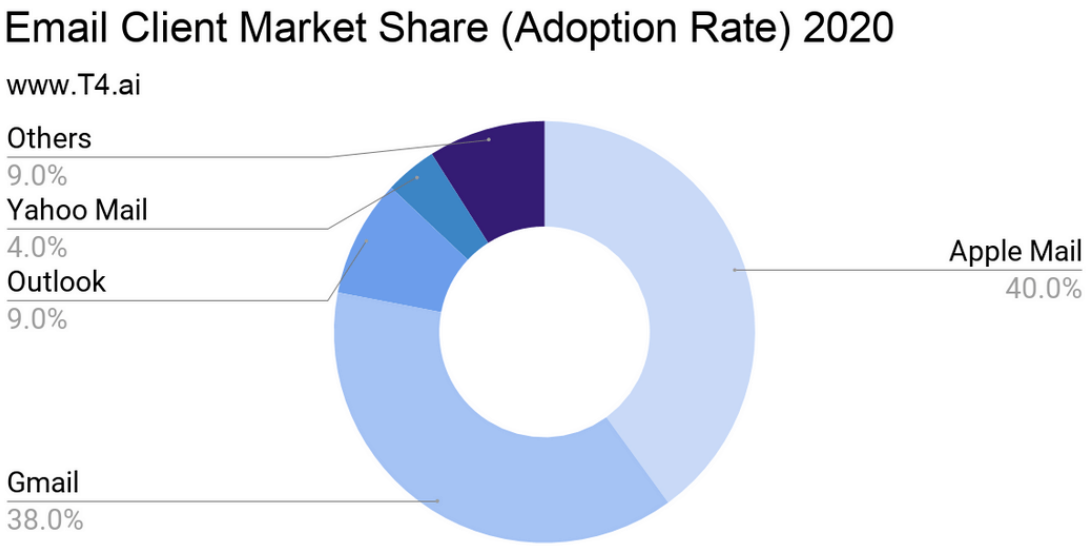

Figure 2 : Répartition des parts de marché dans le domaine des emails

[12] https://www.t4.ai/industry/email-client-market-share

Fort de leur succès aux niveaux de leurs produits hardware, Apple tente maintenant de se faire une place dans le marché des services aux utilisateurs. C'est ce qu'ils ont annoncé au début de l'année 2020 via un article qui s'intitule « Apple entre dans une nouvelle ère de services après une année charnière[13] ».

L'article met en avant les différents services que l'entreprise exploite et expose des statistiques qui permettent de se rendre compte de la puissance de l'entreprise.

Les statistiques avancées concernent notamment l'App Store, le magasin d'application de la firme ou encore Apple News, un service regroupant plusieurs médias en un seul abonnement.

> *Avec plus d'un demi-milliard de visiteurs chaque semaine, l'App Store est le marché d'applications le plus sûr et le plus dynamique au monde.*
>
> *Apple News compte plus de 100 millions d'utilisateurs actifs mensuels aux États-Unis, au Royaume-Uni, en Australie et au Canada et révolutionne la façon dont les utilisateurs accèdent aux articles de leurs sources d'informations préférées.*

Toutes les statistiques exposées ainsi que l'envie d'Apple de proposer de plus en plus de services ne laissent aucun doute sur le fait que l'entreprise va continuer d'occuper une place de choix dans l'écosystème du web. En effet, grâce au nombre faramineux d'appareils de la marque actifs dans le monde et qui utilisent par défaut les services de l'entreprise, on ne peut pas dénier que la dépendance à Apple est très forte et qu'elle risque encore de s'accroître dans les années à venir.

[13] https://www.apple.com/fr/newsroom/2020/01/apple-rings-in-new-era-of-services-following-landmark-year/

2.2.1.3 Facebook

La troisième lettre de l'acronyme, le F, fait référence à Facebook. Le réseau social, créé en 2004, est aujourd'hui le plus utilisé au monde. Pas moins de 2,9 milliards de personnes utilisent le réseau social au moins une fois par mois et quasiment 2 milliards de personnes l'utilisent chaque jour[14].

Facebook est désormais bien plus qu'un simple réseau social comme il l'était lors de son lancement et de ses premières années. L'introduction de nouvelles fonctionnalités et de nouveaux espaces ont constamment changé la façon d'utiliser cet outil

C'est également via l'acquisition de deux entreprises que Facebook s'est créé l'empire que l'entreprise dirige aujourd'hui. La première des deux, en avril 2012, concerne Instagram, application de partage de photos. Facebook rachète alors la jeune entreprise pour une somme d'un milliard de dollars.

En 2021, Instagram compte 1,21 milliard d'utilisateurs actifs et pas moins de 500 millions d'entre eux se rendent sur l'application au moins une fois par jour[15]. Ces chiffres font d'Instagram le 5ème réseau social le plus utilisé actuellement.

La deuxième acquisition qui a permis à Facebook d'asseoir sa mainmise sur les réseaux sociaux, c'est celle de WhatsApp. L'application créée en 2009 a été rachetée 5 ans plus tard par Facebook pour la modique somme de 19 milliards de dollars.

Depuis, l'application n'a cessé d'évoluer afin de lui permettre d'être aujourd'hui l'application de messagerie la plus utilisée au monde avec pas moins de 2 milliards d'utilisateurs[16]. Elle est secondée par Facebook Messenger, la solution de messagerie intégrée à Facebook, qui compte elle 1,3 milliard d'utilisateurs.

Avec ses deux applications de messagerie, Facebook touche donc 3,3 milliards de personnes dans le monde, soit proche de la moitié de la population mondiale.

Ces statistiques prouvent une nouvelle fois que ces entreprises peuvent aujourd'hui être considérées comme des empires. En effet, si l'on considère tous les chiffres avancés, on peut affirmer que les services de Facebook sont utilisés par environ deux personnes sur trois dans le monde.

[14] https://backlinko.com/facebook-users
[15] https://www.oberlo.fr/blog/chiffres-instagram
[16] https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/

2.2.1.4 Amazon

Pour terminer, le deuxième A de l'acronyme correspond à Amazon. L'entreprise américaine, créée en 1994 par Jeff Bezos, était au départ spécialisée dans la vente de livres en ligne.

L'entreprise a ensuite diversifié ses domaines d'activité au fur et à mesure et aujourd'hui il est possible d'obtenir presque tout ce que l'on souhaite sur Amazon. Amazon fait actuellement de l'ombre à tous les commerces de détails grâce à leur stock gigantesque et des délais de livraison de plus en plus courts. En 2020, l'entreprise Amazon représentait à elle seule 45% de la vente sur Internet aux États-Unis[17].

Comme l'explique André Staltz dans son article, Amazon ne cherche pas à faire du profit mais à écraser toute concurrence.

> *Amazon does not focus on making profit. Instead, its mission is to seek market leadership, crushing competitors in the USA. – André Staltz*

C'est ce que l'on peut observer sur le graphique ci-dessous qui représente les revenus des entreprises actives dans le commerce sur Internet. On s'aperçoit que déjà en 2012, Amazon fait complètement cavalier seul et s'échappe loin au-dessus de la concurrence.

Nul doute qu'aujourd'hui, en 2021, cette différence est encore plus importante et Amazon est vraiment seul au monde sur le marché de la vente en ligne.

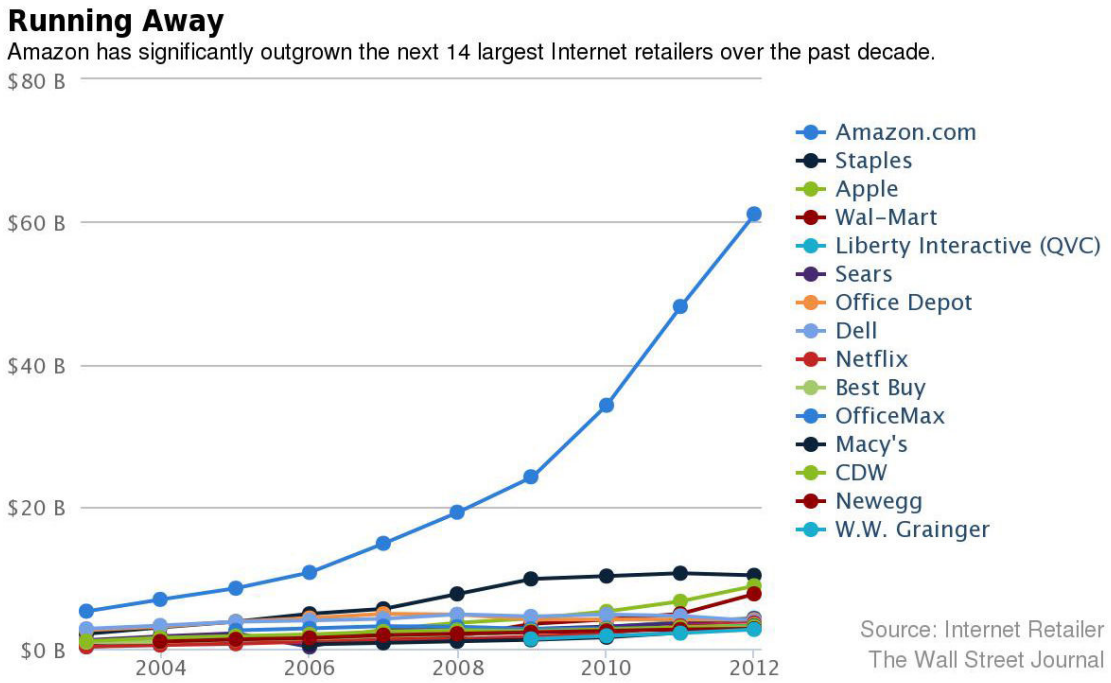

Figure 3 : Revenus des entreprises dans le domaine de la vente sur internet

[17] https://www.repricerexpress.com/amazon-statistics/

Au-delà de son activité principale, Amazon se démarque aussi par des acquisitions et des nouvelles activités importantes qui lui permettent de toucher encore plus de personnes.

C'est le cas notamment du service de streaming Amazon Prime Video créé en 2016 et qui se positionne clairement comme l'un des principaux concurrents du géant Netflix. Amazon annonce en 2021 que son service de streaming comptabilise plus de 200 millions d'abonnés[18]. Ce nombre d'utilisateurs place le service d'Amazon juste derrière Netflix avec ces 207 millions d'utilisateurs à la fin du premier trimestre 2021[19].

Au niveau des acquisitions de l'entreprise, deux sortent particulièrement du lot. La première des deux concerne Twitch, la plateforme de streaming de jeux vidéo en ligne. Amazon a acquis la plateforme en août 2014 pour une somme approchant le milliard de dollar. Leur flair a été bon car aujourd'hui Twitch comptabilise environ 140 millions d'utilisateurs mensuels dont 15 millions sont actifs chaque jour[20]. L'entreprise a également rapporté 1.5 milliard de dollars à Amazon en 2019[21].

La deuxième acquisition, la plus récente des deux, vise à asseoir la place d'Amazon dans le secteur du divertissement. Amazon a en effet acquis Metro-Goldwyn-Mayer, société de production extrêmement connue et respectée dans l'industrie cinématographique. La transaction a eu lieu en mai 2021 pour la somme de 8.45 milliards de dollars.

Cette acquisition couplée au développement des propres studios de production cinématographique de la firme, Amazon Studios, doit permettre au service de streaming Amazon Prime Video de s'imposer à terme comme le leader incontesté du domaine aujourd'hui dominé par le concurrent Netflix.

Les chiffres exposés pour Amazon montrent une nouvelle fois la puissance de ces entreprises composant ces géants du web. Amazon a en effet une mainmise complète sur la vente de détail en ligne et les parts de l'entreprise ne font qu'augmenter.

[18] https://www.fool.com/investing/2021/04/27/amazon-reaches-200-million-prime-member-milestone/
[19] https://www.statista.com/statistics/250934/quarterly-number-of-netflix-streaming-subscribers-worldwide/
[20] https://mediakix.com/blog/top-twitch-statistics-live-streaming-game-platform/
[21] https://www.pcgamesn.com/twitch-youtube-gaming-2019-revenues

2.2.1.5 Autres entreprises

Nous avons abordé les quatre entreprises qui composent les GAFA mais il serait possible d'en ajouter d'autres.

On peut notamment citer Netflix et Microsoft. Netflix car c'est le leader mondial du streaming vidéo sur Internet. C'est eux qui ont popularisé cette nouvelle façon de consommer du contenu et avec plus de 200 millions d'utilisateurs, cela fait d'eux une entreprise avec un fort pouvoir sur le web.

Microsoft, comme Apple, n'est pas une entreprise directement spécialisée dans le domaine du web. En effet, leur produit phare concerne plutôt les systèmes d'exploitation. On parle ici bien sûr de Windows qui équipe environ 76% du parc mondial informatique de bureau[22].

Ils cherchent également à se faire une place sur le web, en ayant notamment mis en place un moteur de recherche, un outil de cartographie ou encore Outlook, le service de mail de Microsoft.

Malgré ces efforts, l'entreprise reste en retrait par rapport aux autres géants du web mais elle a tout de même un fort pouvoir grâce à la popularité et l'utilisation de ses systèmes d'exploitation.

On peut également mêler dans le combat une autre catégorie d'entreprises bien précises, celles qui ont cassés un modèle économique qui existait déjà en le numérisant complètement. On peut citer Airbnb, qui a révolutionné la façon de louer ses biens immobiliers à travers le monde. Uber a également complètement révolutionné un segment de marché en s'attaquant au monopole des taxis dans les villes.

Ces entreprises ont du pouvoir mais il reste limité par rapport aux autres géants du web. En effet, ils peuvent agir sur leur domaine d'activité en particulier mais ils ne possèdent pas d'empire leur permettant de modifier de manière globale la façon d'utiliser le web.

[22] https://gs.statcounter.com/os-market-share/desktop/worldwide

2.2.2 Les données

Les données sont le nerf de la guerre pour ces géants du web. C'est grâce à nos données qu'ils produisent la majorité de leurs revenus. Par exemple en 2017, Facebook a récolté pas moins de 98% de ses 40 milliards de revenus annuels grâce à nos données[23].

Mais alors pourquoi ces données sont-elles importantes et surtout qu'est-ce que les entreprises en font ?

Grâce à nos données personnelles, souvent demandées lors de notre inscription, ainsi que notre activité sur le site en question, les algorithmes de l'entreprise sont capables de dresser un profil de chaque utilisateur.

Ce profil contient nos informations personnelles, telles que notre âge, notre sexe ou encore la zone dans laquelle nous habitons. Il contient également notre métier, nos centres d'intérêts ou encore nos goûts en matière de musique ou alors de cinéma.

Ces informations concernant notre personnalité et nos intérêts sont particulièrement intéressantes pour le site lui-même car il lui permet d'adapter son offre afin qu'elle nous corresponde le plus possible et nous incite à rester plus longtemps.

Les plus intéressés par ces millions de profils détaillés, ce sont les annonceurs publicitaires. En effet, il paraît logique qu'une personne intéressée par le bricolage aie plus de chance d'acheter une perceuse dans les 6 prochains mois qu'une personne qui n'a jamais fait aucune recherche sur ce sujet.

Google, Facebook et Amazon revendent ces profils aux annonceurs qui paient des fortunes afin de savoir à quels utilisateurs leurs annonces ont le plus de chance d'aboutir. Apple est la seule entreprise qui apparemment ne revend pas les données de ses utilisateurs. Selon eux, ils les utilisent uniquement pour améliorer leurs services ainsi que les applications disponibles sur leurs appareils.

C'est pour cette raison que les publicités que nous recevons par exemple sur Facebook semblent la plupart du temps être presque magiques tellement elles sont pertinentes.

Ces reventes d'informations, que nous acceptons de notre plein gré lorsque nous créons des comptes, représentent une atteinte à la vie privée des utilisateurs car cette dernière est exposée au grand jour.

[23] https://www.youtube.com/watch?v=2h86lnDv2PQ

Le danger, c'est également les fuites et vols de données. Nous n'avons pas d'autres choix que de faire confiance à ces géants du web concernant les données que nous leur fournissons et que nous générons avec notre activité.

Ces données sont stockées dans de gigantesques centres de données qui fleurissent à travers le monde. Cette quantité astronomique de données est souvent référée sous le nom de *big data*. Le problème de ces centres de données, c'est qu'ils sont connectés à Internet. Et malgré toutes les précautions du monde, un serveur connecté à Internet est attaquable et présente des vulnérabilités.

Il est donc malheureusement probable que nos données soient volées ou alors se retrouvent dans la nature par mégarde. Cela arrive malheureusement encore souvent et concerne des informations personnelles qui devraient rester secrète et qui peuvent ensuite être utilisées contre nous.

2.2.3 Les conditions d'utilisation

Lors de nos inscriptions sur les sites des géants du web, nous cochons tous la petite case « j'accepte les conditions d'utilisation » alors que nous n'avons même pas lu les informations que ce document contient.

Ces documents font souvent plusieurs dizaines de pages et contiennent beaucoup d'informations légales peu intéressantes pour l'utilisateur. Toutefois, ces documents contiennent certaines parties qui concernent l'utilisation de nos données et les droits que nous accordons à l'entreprise en acceptant ces conditions.

On apprend par exemple en lisant les conditions d'utilisation de Facebook que :

> *Lorsque vous partagez, publiez ou importez du contenu protégé par des droits de propriété intellectuelle sur ou en rapport avec nos Produits, vous nous accordez une licence non exclusive, transférable, sous-licenciable, gratuite et mondiale pour héberger, utiliser, distribuer, modifier, exécuter, copier, représenter publiquement ou afficher publiquement, traduire et créer des œuvres dérivées de votre contenu.*

Cette phrase montre bien que le contenu que nous mettons en ligne sur Facebook ne nous appartient plus vraiment.

Ces conditions, nous les acceptons tous de notre plein gré lors de notre inscription. Nous n'avons pas réellement le choix car si nous les refusons, nous ne pouvons pas utiliser le produit mis à disposition par l'entreprise.

Le réel problème concernant ces conditions, c'est que ces entreprises ont la fâcheuse tendance de beaucoup les modifier et d'ajouter de plus en plus de contenu. Ce nouveau contenu, que la plupart des gens ne lisent pas une nouvelle fois, nous l'acceptons sans même réfléchir lorsque l'annonce s'affiche à notre retour sur le produit.

Cela pose problème car les entreprises peuvent faire quasiment ce qu'elles veulent. En effet, nous avons souvent besoin de leur produit pour notre activité professionnelle ou alors notre vie privée. Cela ne nous permet donc pas de se passer de ces produits et nous devons donc en accepter les conditions sans sourciller.

Nous sommes donc quelque peu prisonniers car peu importe les nouvelles conditions mises en place par une entreprise, nous allons les accepter car ne pas utiliser leur produit n'est pas une alternative possible tellement leur emprise est grande sur l'écosystème global du web.

2.2.4 L'infrastructure

Comme expliqué plus tôt dans ce travail, mettre un site à la disposition du public est une tâche relativement simple qui peut être réalisée depuis n'importe quel ordinateur.

Cependant, si plusieurs utilisateurs utilisent votre service et que les données commencent à s'empiler, des problèmes de performances vont rapidement survenir. Si vous souhaitez que votre site soit accessible 24 heures sur 24, votre appareil doit également rester allumer sans arrêt.

La question de la rapidité de la connexion à internet est également un problème majeur de l'auto-hébergement à la maison. En effet, il est maintenant normal d'avoir une grande capacité de téléchargement mais les vitesses de téléversement restent relativement faibles. Cela va donc ralentir l'accès à votre site, surtout si plusieurs connexions simultanées sont établies.

C'est pourquoi, si l'on souhaite que son service prenne son envol et accueille de plus en plus de clients, il va falloir se tourner vers un hébergement dans un centre de données. Il est certes possible de se tourner vers un hébergeur local, par exemple *Infomaniak* à Genève, mais nous parlons ici d'entreprises qui souhaitent s'ouvrir au marché mondial.

Pour héberger son site internet, il va alors falloir se tourner vers les géants de l'hébergement sur internet. Et là, lorsque l'on s'intéresse aux trois principaux leaders du domaine, on s'aperçoit que ce n'est autre que Amazon, Microsoft et Google.

Après avoir pris le contrôle des services destinés aux utilisateurs classiques, ces 3 entreprises se sont attaquées aux services pour les professionnels du web.

Ils ont à eux trois pris le contrôle de ce domaine car on s'aperçoit en analysant l'argent dépensé par les clients dans ce domaine, que ces 3 acteurs accaparent 58% de ce montant[24]. Ce pourcentage énorme se partage de la façon suivante :

- 32% pour AWS (Amazon Web Services)
- 19% pour Microsoft Azure
- 7% pour Google Cloud

[24] https://www.canalys.com/newsroom/global-cloud-market-Q121

L'avance d'Amazon dans le secteur s'explique par l'année de création des services. Amazon Web Services a en effet pris son envol en 2006 alors qu'Azure date de 2010 et Google Cloud de 2011. Selon Jeff Bezos, CEO d'Amazon, c'est la principale raison de cette mainmise sur le domaine :

> *AWS had the unusual advantage of a seven-year head start before facing like-minded competition. As a result, the AWS services are by far the most evolved and most functionality-rich. – Jeff Bezos*

En conclusion, si l'on souhaite aujourd'hui proposer à ses utilisateurs une application web qui va réussir à suivre ses concurrents au niveau de la disponibilité, des performances et de la capacité de stockage, il faudra obligatoirement passer par les services de l'un des trois géants américains.

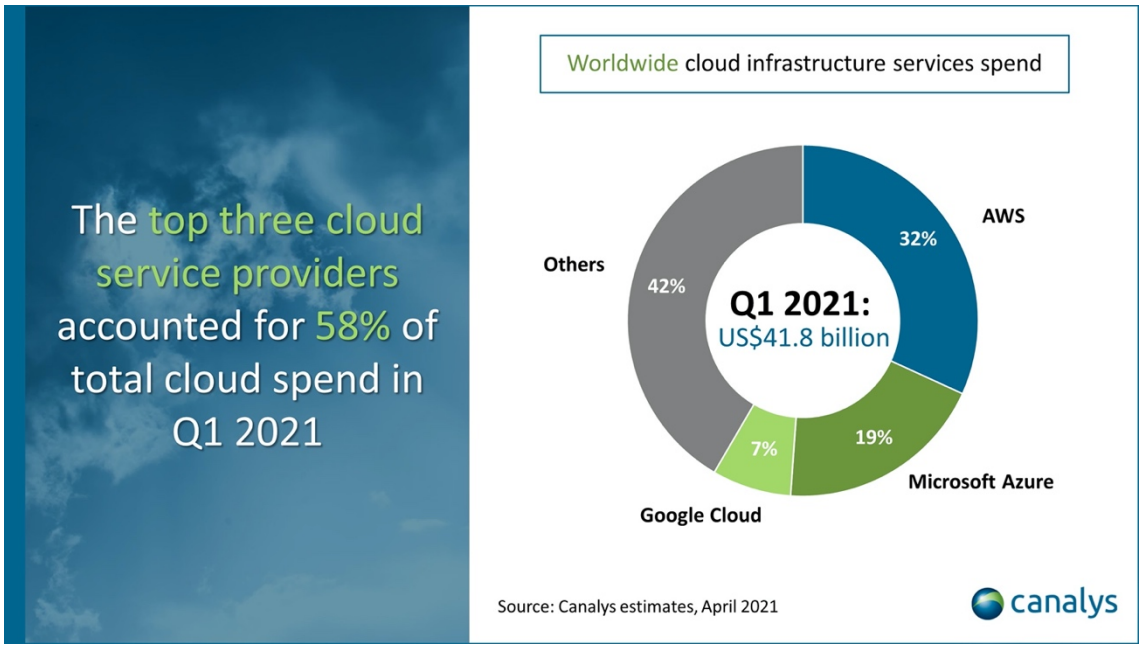

Figure 4 : Montant dépensé dans le cadre des services d'hébergement

2.3 Le pouvoir des gouvernements

La structure actuelle du web et par extension la structure de l'infrastructure physique d'internet facilite malheureusement le contrôle des gouvernements sur le web. Ces contrôles, qui peuvent aller de la simple censure de site web à une surveillance radicale des utilisateurs va à l'encontre même des fondements du web qui se veut comme un espace libre et démocratique.

Quatre types de censures existent sur le web :

- Censure politique
- Censure religieuse
- Censure sécuritaire
- Censure commerciale

L'objectif des gouvernements avec la censure politique c'est de réduire au silence les opposants au gouvernement mis en place. Ces opposants peuvent se trouver soit directement à l'intérieur du pays soit être des pays étrangers que le gouvernement considère comme ennemis. Ce type de censure est très présent dans les dictatures que l'on trouve encore malheureusement à travers le monde.

Le deuxième type de censure, c'est la censure religieuse. Comme son nom l'indique, cette dernière cherche à réduire à néant l'accès à l'information concernant les religions autre que celle qui est pratiquée majoritairement dans le pays en question. Cette censure est très présente dans les pays arabes qui restent majoritairement opposés à la pratique d'autres religions.

La troisième est une censure sécuritaire. Cette censure cherche à garder le pays en question sûr en censurant d'éventuelles plateformes ou sites qui pourrait nuire à sa sécurité intérieure.

Enfin, le dernier type de censure est commercial. Cette censure cherche à empêcher l'accès à des produits que le gouvernement ne souhaite pas autoriser sur son territoire. Cela peut concerner des produits de toutes sortes mais c'est le plus souvent des produits électroniques qui sont concernés.

Les gouvernements des pays peuvent mettre en place ces censures de différentes manières. Le plus simple pour un gouvernement totalitaire, c'est de définir un point d'accès unique au réseau internet. Ce point unique est accessible uniquement par un opérateur que le gouvernement contrôle. De cette manière, il est possible de filtrer toutes les connexions entrantes et sortantes afin de ne pas laisser passer ce qui ne convient

pas au gouvernement. C'est la manière de faire qu'utilise la Chine ou encore l'Iran afin de garder la mainmise sur l'utilisation du web par leurs citoyens.

La deuxième technique, déjà abordée en introduction de ce chapitre, consiste à retirer les enregistrements voulus des serveurs DNS du fournisseur d'accès à Internet. De cette manière, l'utilisateur ne pourra pas récupérer l'adresse IP qui correspond au nom de domaine qu'il recherche.

Cette méthode est toutefois perfectible car quasiment tous les appareils disposant d'une connexion à Internet permettent de changer le serveur DNS si on le souhaite. Ainsi en utilisant un DNS libre, l'utilisateur pourra récupérer l'adresse IP du serveur qu'il souhaite atteindre.

Une méthode permettant de complètement condamner l'accès au site consiste à demander aux fournisseurs d'accès à Internet de filtrer les adresses IP des paquets qui transitent par leurs équipements. Ainsi, si un paquet vient d'un site qui est inscrit sur une liste noire, il est intercepté lors du routage chez l'opérateur et il n'arrivera jamais jusqu'à l'utilisateur final.

Si cette méthode est mise en place par un opérateur, sur demande du gouvernement, l'utilisateur ne pourra malheureusement jamais accéder au site web qui l'intéresse.

Enfin, une dernière méthode plus douce et facile à contourner consiste à retirer les résultats concernant une certaine recherche dans les moteurs de recherche. Cette méthode affectera les utilisateurs les moins persistants mais ne permettra pas de complètement bloquer l'accès à un certain site.

On pourrait penser que ces censures sont présentes uniquement dans des pays totalitaires lointains mais ce n'est pas du tout le cas, comme on peut s'en rendre compte en consultant cette carte.

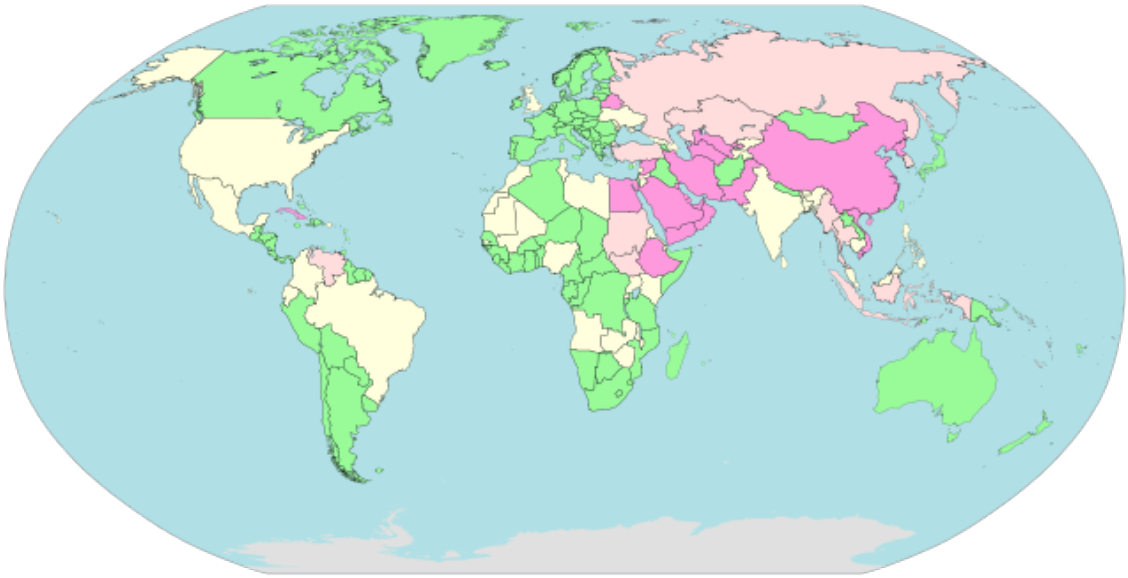

Figure 5 : Niveau de censure et surveillance par pays

Cette carte se base sur les données de l'OpenNet Initiative récoltées entre 2004 et 2014[25]. Cette initiative cherche à étudier le filtrage d'internet, autrement dit la censure, et la surveillance des différents gouvernements sur Internet.

Le rose foncé représente une censure ou surveillance forte et le rose clair représente une censure ou surveillance partielles. Les pays représentés en jaune clair mettent en place une censure ou surveillance sélective. Enfin, les pays en vert représentent les bons élèves car ce sont les pays qui comportent quelques censures ou alors une censure inexistante.

[25] https://opennet.net/research/data

Nous avons beaucoup parlé de censure car il est facile de vérifier si des sites sont accessibles ou non dans certains pays. Il est par contre plus difficile de savoir si les utilisateurs d'un certain pays sont surveillés ou non.

La surveillance peut être générale, c'est-à-dire que le gouvernement a une trace des faits et gestes de tous ses concitoyens ou alors une surveillance ciblée sur quelques individus. Si nous n'avons pas de preuves tangibles concernant une quelconque surveillance des gouvernements actuellement, il ne fait aucun doute que ces derniers ont accès dans une certaine mesure à nos activités sur internet.

Ce doute qui persistait a été complètement effacé par les révélations d'Edward Snowden en 2013. Dans les nombreux documents qu'il a rendu public, on apprend que les États-Unis sont capables de surveiller quasiment n'importe qui sur Internet mais aussi sur les téléphones portables et autres moyens de communications.

Ces révélations ont bien sûr eu l'effet d'une bombe et ont renforcé la méfiance des utilisateurs envers les différents gouvernements qui officiellement ne surveillent pas leur population.

En conclusion, la censure ainsi que la surveillance du web sont des problèmes qui n'atteignent pas que les dictatures mais bel et bien le monde entier. Le web devrait être un espace de liberté où la liberté d'expression est le maitre mot mais avec le contrôle incessant et intrusif des gouvernements, cela est malheureusement loin d'être le cas.

2.4 Explication du problème

Nous avons beaucoup parlé de ces grandes entreprises à l'aide de statistiques qui montrent leur puissance sur le domaine du web mais au fond, pourquoi cela pose-t-il un problème ?

Jusqu'à récemment, cela ne posait pas réellement de problème. En effet, les entreprises en question sont douées dans leurs domaines et l'écosystème fonctionnait alors normalement.

Cependant, avec la puissance accumulée, le pouvoir monte rapidement à la tête et ces entreprises en veulent toujours plus afin de contrôler et de façonner le web de la façon qu'ils le souhaitent.

Toutes les entreprises n'ont pas les mêmes vices mais on peut en citer au moins un pour chacune des quatre entreprises composant les GAFA.

Pour Google, c'est l'acquisition incessante d'entreprises qui cherchent à les concurrencer qui commence à faire grincer des dents dans la Silicon Valley et au-delà. Dès que l'entreprise a vent d'un produit qui pourrait concurrencer leurs services, ils l'achètent et incorporent les bonnes idées au sein de leurs propres produits. Les petites entreprises concernées acceptent le plus souvent les propositions d'achat car elles les montants sont élevés et leur permettent de s'assurer un futur qui était incertain.

Pour Amazon, ce sont principalement les conditions de travail qui sont au centre des discussions. Dans leurs nombreux entrepôts, les employés doivent travailler extrêmement rapidement durant de longues heures et avec peu de pauses. De plus en plus d'employés se plaignent en espérant que cela pousse l'entreprise à revoir ses conditions de travail. On peut par exemple prendre l'exemple d'un centre de tri de paquets à New York. Dans ce centre, les employés doivent inspecter et scanner les paquets qui passent devant eux. Chaque employé doit prendre en charge 1800 paquets par heure, ce qui représente un toutes les 2 secondes[26].

Cette activité s'effectue pendant 12 heures d'affilées avec seulement deux pauses de 15 minutes chacune. Ces conditions stressantes et fatigantes ainsi qu'une augmentation des accidents de travail ont amenés les employés à signer une pétition adressée à leurs employeurs afin que les conditions s'améliorent. Ce n'est qu'un exemple parmi d'autres car les conditions sont les mêmes partout.

[26] https://www.theguardian.com/technology/2020/feb/05/amazon-workers-protest-unsafe-grueling-conditions-warehouse

Pour Facebook, c'est la gestion et l'utilisation des données personnelles de ses utilisateurs qui est au centre de toute l'attention. En effet, la façon d'utiliser les données ainsi que les nombreuses reventes à d'autres entreprises a considérablement affecté l'image de l'entreprise auprès des utilisateurs.

A cela s'ajoute également les scandales de nature géopolitique, dont le plus connu est sans équivoque Cambridge Analytica. Cette entreprise a exploité les données 87 millions d'utilisateurs de Facebook afin d'influencer les utilisateurs dans leurs décisions politiques[27].

Cette révélation a indigné tous les milieux et malgré les excuses de Facebook, leur image s'est vue extrêmement affectée et la valeur de l'entreprise en bourse a chutée.

Pour Apple, ce sont les conditions de travail des nombreuses usines asiatiques qui fabriquent les nombreux appareils de la marque qui sont au cœur du problème. L'entreprise essaie bien d'établir des règles que les fournisseurs doivent suivre mais ces derniers n'ont pas le choix que de violer ces règles afin de pouvoir suivre la cadence extrême voulue par Apple afin d'avoir assez d'appareils disponibles à la vente.

Les conditions de travail sont par endroit inhumaines à cause des heures de travail demandées et du travail lui-même qui est souvent extrêmement précis et contient des opérations qui peuvent être dangereuses pour la personne qui les exécute. Ces conditions ainsi que les salaires extrêmement bas pousse malheureusement un nombre significatif de ces travailleurs au suicide. Les images de filets ajoutés aux bâtiments afin de prévenir les suicides font froid dans le dos[28].

Ces raisons sont les principales qui amènent les utilisateurs à de plus en plus se méfier de ces grandes entreprises. Ce sont aussi ces raisons qui posent un problème éthique quant à la superpuissance de ces entreprises alors que derrière leurs belles promesses, elles ne sont pas vraiment exemptes de tout reproches.

[27] https://fr.wikipedia.org/wiki/Scandale_Facebook-Cambridge_Analytica
[28] https://www.theguardian.com/technology/2017/jun/18/foxconn-life-death-forbidden-city-longhua-suicide-apple-iphone-brian-merchant-one-device-extract

Au-delà des problèmes énoncés dans ce chapitre, cette trop grande centralisation du web a mis un frein complet à l'innovation. En effet, les innovations n'arrivent jamais jusqu'aux utilisateurs si elles ne sont pas implémentées dans les produits des géants.

Le web devait être à la base un espace d'innovation constant et florissant mais ce n'est aujourd'hui plus du tout le cas. Il est impossible de se faire une place au soleil dans l'écosystème si l'on ne fait pas partie d'un des géants.

Pour prouver ce point, il suffit de se demander depuis quand nous n'avons plus vu un nouvel arrivant bouleverser l'écosystème et se faire une place sur le web. La dernière entreprise qui a réussi cet exploit, c'est Snapchat. Sa création datant de 2011, cela fait donc 10 ans que nous n'avons plus vu un nouvel acteur s'imposer sur le web alors que les idées ne manquent pas.

En conclusion, il est une évidence que cette ultra-domination des géants du web n'est pas saine. Autant d'un point de vue éthique que concernant l'innovation et la liberté sur le web, ces points qui semblent essentiels ne sont aujourd'hui pas acquis.

3. Les solutions possibles

Comme nous l'avons vu dans le chapitre précédent, les problèmes liés à la centralisation du web sont multiples. En effet, les gouvernements qui censurent, les GAFA qui freinent l'innovation ou encore l'éthique discutable des géants du domaine pèsent sur le web et polluent un espace qui devrait être dédié à la liberté.

Nous allons maintenant nous intéresser aux différentes solutions techniques qui permettraient de remettre le pouvoir sur le web dans les mains des utilisateurs.

3.1 Solutions techniques

3.1.1 Auto-hébergement

La grande majorité des sites web que l'on consulte chaque jour sont hébergés sur des serveurs qui sont physiquement installé dans des grands centres comprenant plusieurs centaines voire milliers de serveurs, que l'on appelle des centres de données.

Lorsque l'on accède à ces sites, on demande des informations à un serveur qui nous les renvoie et ensuite notre navigateur se charge de nous les présenter à l'écran.

On peut prendre l'exemple d'un service de messagerie en ligne, comme par exemple Gmail. Lorsque l'on veut aller vérifier si on a reçu du courrier, on se connecte sur le site gmail.com. Lorsque l'on tape cette adresse dans notre navigateur, on va se connecter à l'un des serveurs de Google qui héberge le service Gmail.

On va ensuite relever le courrier puis ce dernier sera affiché dans notre boite de réception et nous pourrons le consulter. Jusqu'à ce que le courrier soit relevé, c'était donc le serveur de Google qui gardait en attente notre courrier.

Le problème, c'est qu'il est possible d'effectuer des actions sur ce courrier avant qu'il n'arrive jusqu'à nous. Il est par exemple possible de filtrer selon plusieurs mots clés ou encore d'analyser le contenu afin de nous proposer des publicités plus ciblées.

Autrement dit, nos messages, qui peuvent être confidentiels, sont stockés sur un serveur dont nous ignorons la localisation géographique et dont nous ignorons également à quel point notre contenu est scruté et analysé.

L'une des solutions, c'est d'héberger soi-même chez soi le serveur auquel on va se connecter pour récupérer nos messages.

Il n'est bien sûr pas possible d'héberger un serveur Gmail chez soi, l'idée est plutôt de mettre sur pied un service qui nous appartient et qui nous permet d'envoyer et de recevoir des mails sans devoir faire confiance à une entreprise externe.

Cela demande bien sûr un effort d'installation et de configuration car il va falloir mettre en place un serveur sur une machine chez soi. Un effort devra également être fait afin de sécuriser le serveur pour que nos données ne se retrouvent pas dans la nature par accident.

Le principal avantage, c'est que vos données sont chez vous et vous appartiennent. Elles sont stockées sur le disque dur de votre machine et vous pouvez donc en faire ce que vous en souhaitez. Si vous décidez de supprimer du contenu, ce dernier sera réellement supprimé et il ne restera pas une copie sur un serveur distant.

Un autre avantage de taille réside dans le fait que grâce au fait que les données sont hébergées chez nous, notre vie privée est respectée. Nos données ne seront pas scannées puis analysées afin de dresser un profil de nos centres d'intérêts ou alors de nous proposer de la publicité ciblée.

L'auto-hébergement représente également un bon exercice afin de s'instruire sur le fonctionnement d'internet et du web en général. En mettant en place un service chez soi, on acquiert des compétences et une connaissance du web qui peuvent s'avérer importantes dans un monde toujours plus connecté.

Il n'y a bien sûr pas que des avantages à l'auto-hébergement, sinon tout le monde le ferait déjà. Le plus gros inconvénient, c'est qu'en hébergeant vos propres services, vous faites une croix sur toutes les fonctionnalités puissantes qu'offrent les services des géants du web.

En effet, le service que vous allez installer chez vous remplira son rôle mais sera à coup sûr moins pratique, moins puissant et très probablement moins joli et facile d'utilisation. Néanmoins, c'est un sacrifice qu'il faut être prêt à faire si on veut retrouver le contrôle de nos données et donc une vie privée qui est respectée.

Il existe également quelques autres inconvénients, notamment le fait que mettre en place et tenir à jour la machine qui héberge les services est une activité qui prend du temps. La bande passante que votre connexion domestique peut fournir est également limitée, le service sera donc probablement plus lent que si vous y accédiez via un centre de données. Pour un service de mail, la différence sera minime mais si vous souhaitez héberger un service qui doit gérer des grandes quantités de données, par exemple un service de partage de fichiers, la différence sera notable.

Enfin, la machine qui héberge vos services doit rester allumée sans interruption. En effet, si quelqu'un vous envoie un message et que votre serveur est éteint, ce message ne vous parviendra jamais car il n'existe pas d'intermédiaire qui peut garder votre message en attente avant de vous le délivrer lorsque vous allumez votre serveur.

Il faut donc prévoir un espace où entreposer sa machine afin qu'elle reste allumée, si possible, tout le temps. Cela peut donc également influer sur votre facture d'électricité mais il est maintenant possible d'utiliser du matériel à faible consommation électrique, ce qui transforme donc cet inconvénient en une opportunité.

Vous pouvez en effet investir dans du matériel à faible consommation et ainsi participer à l'effort général pour faire attention à la planète tout en préservant votre vie privée et en contribuant à la décentralisation du web.

Dans ce chapitre, j'ai pris l'exemple d'un service de messagerie afin d'illustrer le fonctionnement et les avantages de l'auto-hébergement mais il est possible d'héberger des services de toutes sortes chez soi.

Cela peut aller du partage de fichiers à l'hébergement de vidéos en passant par votre propre service de streaming (musical et vidéo) ou encore l'hébergement de vos sites web, les possibilités sont nombreuses.

Au niveau de la faisabilité de l'auto-hébergement, cette dernière est très haute. Toutes les personnes possédant un ordinateur à la maison et souhaitant mettre en place un service chez soi sont capables de le faire. Cela est même tout à fait possible sans grandes connaissances du domaine car un grand nombre de tutoriels existent sur le web et expliquent en détail la mise en place de ces services.

L'auto-hébergement représente donc, pour ceux qui le souhaitent, une très bonne alternative à certains services qui sont proposés par les géants du web. Il permet de reprendre le contrôle de ses données, sans pour autant faire une croix sur les services que peut proposer le web, tout en contribuant à une décentralisation progressive de ce dernier.

3.1.2 P2P

Une autre solution, c'est de construire sur les bases d'une technologie déjà existante afin d'obtenir un réseau complètement distribué. Cette technologie, c'est le P2P (peer-to-peer).

L'idée du P2P c'est de se passer du modèle habituel client-serveur où le serveur est le seul à stocker l'information et il la communique aux clients lorsque ceux-ci le demandent.

Avec le P2P, tous les utilisateurs font office de client et de serveur. Lorsque l'on connecte son appareil à un réseau P2P, on devient alors un nœud de ce réseau. Ce nœud est ensuite capable d'agir en tant que client, c'est-à-dire de recevoir des données et en tant que serveur, c'est-à-dire d'envoyer des données à d'autres clients du même réseau.

Le principe du P2P est principalement utilisé actuellement pour le partage de fichiers entre utilisateurs. Le principal protocole utilisé est BitTorrent.

Le principe de BitTorrent est relativement simple. Lorsqu'une information, dans notre cas représentée par un fichier, est stockée sur un serveur unique et qu'elle est beaucoup demandée, elle devient alors moins accessible à cause du nombres de connexions.

Afin d'éviter ce problème, chaque client qui est en train de télécharger le fichier devient alors à son tour serveur pour ce fichier, le serveur original est alors déchargé et les débits peuvent être plus rapides.

Afin de gérer comment le fichier est partagé et de s'assurer qu'il soit entier, chaque fichier est séparé en un certain nombre de segments. Le protocole s'occupe ensuite de diffuser ou alors de télécharger ces segments entre les différents nœuds du réseau afin que le maximum de personnes puisse obtenir le fichier complet aussi rapidement que possible.

Une fois le fichier complètement téléchargé, le système continuera d'envoyer des segments de celui-ci aux nouveaux clients qui ne les ont pas encore. Une fois le fichier téléchargé chez ces nouveaux clients, ces derniers rejoignent alors un nombre grandissant de serveurs qui proposent ce fichier aux nouveaux clients.

De cette manière, la disponibilité du fichier est assurée en tout temps et les vitesses de téléchargement sont nettement accélérées. Il n'existe également aucun point de défaillance unique car le fichier est accessible via plusieurs serveurs qui n'ont pas de liens entre eux.

Le seul problème intervient lorsque plus personne ne partage le fichier original. Dans ce cas-là, lorsqu'on essaie de télécharger le fichier, ce dernier restera bloqué à 0% en nous indiquant qu'il ne trouve pas de source.

La force du protocole permet toutefois à une personne qui stocke toujours le fichier sur son ordinateur mais qui a arrêté de le partager de devenir à nouveau une source. En effet, en téléchargeant le fichier .torrent original, l'application va contrôler que tous les segments du fichier sont corrects via un hash puis si c'est le cas, le fichier va à nouveau être partagé via le protocole.

Actuellement, les principaux fichiers qui sont partagés légalement via ce protocole sont les distributions Linux misent à disposition par différentes entreprises ou privés.

Ce protocole est également très utilisé pour partager du contenu multimédia de manière pas toujours légale selon les pays. Sa décentralisation et son nombre important d'utilisateurs permettent toutefois de s'assurer que les fichiers soient toujours disponibles, peu importe si la personne qui l'a partagé à l'origine agisse toujours comme source ou non.

La deuxième grande application basée sur le P2P concerne le calcul distribué. Le principe est de diviser des calculs complexes en plusieurs parties qui seront effectuées séparément par les ordinateurs connectés au réseau. De cette manière, on démultiplie la puissance de calcul et il sera possible d'arriver plus rapidement à la solution finale.

Plusieurs projets utilisent le principe du P2P afin de proposer un réseau complètement décentralisé. Nous allons ici en passer plusieurs en revue.

3.1.2.1 ZeroNet

ZeroNet est un bel exemple de ce qu'il est possible d'accomplir grâce aux principes du P2P. Le réseau, fondé en 2015 en Hongrie, cherche à promouvoir un web entièrement décentralisé. Ce réseau est bien sûr open-source afin que qui que ce soit puisse consulter et se faire son avis sur le code utilisé. Le réseau est également gratuit, sécurisé et son principal but est d'être incensurable.

Le fonctionnement de ce réseau est très intéressant et pourrait poser des bases solides pour construire un web décentralisé qui appartient au peuple. Pour accéder à un site, au lieu de consulter une adresse IP, l'adresse est identifiée par une clé publique unique.

Ce système rappelle bien sûr les crypto monnaies qui utilisent également ce principe d'adresses publiques pour échanger leurs monnaies.

Lorsque l'on accède à l'un des sites, via sa clé publique, un tracker centralisé va renvoyer la ou les adresses IP qui hébergent le contenu du site. ZeroNet permet ensuite d'échanger un fichier JSON qui contient des données qui permettent de s'assurer que l'échange est sécurisé.

Ce fichier JSON contient un inventaire des fichiers qui composent le site, des hashs permettant de vérifier que les fichiers sont corrects et la clé du propriétaire original du site.

ZeroNet s'occupe ensuite de vérifier que les clés sont correctes puis si c'est le cas, les fichiers qui composent le site seront alors téléchargés et le site pourra être affiché à l'utilisateur.

Une fois que l'on a accédé à un site, on devient alors un seed de ce dernier, ce qui veut dire que d'autres personnes qui accèdent à ce site le feront via le site qui est stocké sur notre ordinateur. Afin de ne pas surcharger de données les ordinateurs des utilisateurs, chaque site peut héberger au maximum 10 Mo sur un ordinateur. Il est possible de dépasser cette limite mais il faut obligatoirement demander l'autorisation de l'utilisateur.

Afin que l'auteur original du site puisse modifier le contenu qui s'y trouve, il peut signer des changements grâce à sa clé privée et ces derniers vont ensuite se propager sur le réseau jusqu'à toutes les machines qui stockent des fichiers de ce site.

Cette manière de faire permet qu'un site soit toujours accessible tant qu'au moins un ordinateur qui l'a un jour visité est allumé et connecté au réseau. Par extension, il est impossible à qui que ce soit de rendre inaccessible un site qui est toujours hébergé quelque part.

Au-delà de la partie P2P, ZeroNet permet également d'accéder et d'héberger des sites web du domaine .bit. Ce nom de domaine un peu particulier est uniquement accessible depuis un serveur DNS alternatif appelé Namecoin.

Un serveur DNS dit alternatif est un serveur qui n'est pas administré par l'ICANN, l'Internet Corporation for Assigned Names and Numbers[29]. Cette société à but non lucratif, basée en Californie, s'occupe d'attribuer les adresses IP au niveau mondial ainsi que de la gestion de tous les domaines DNS dit de premier niveau, tels que par exemple .com, .fr ou encore .ch.

L'ICANN s'occupe d'administrer 13 serveurs DNS racinent qui redirigent les requêtes vers d'autres serveurs spécialisés dans un domaine en particulier.

Le serveur DNS Namecoin repose lui sur une chaîne de bloc clé/valeur qui permet d'enregistrer les noms de domaine de manière décentralisée et sans possibilité d'altérer les informations. Ce système permet d'obtenir des noms de domaines très résistants à la censure car la chaîne de blocs garantit que seul le possesseur de clé privée originale qui a été utilisée pour créer le domaine peut gérer ce dernier.

Pour revenir à ZeroNet, il n'est malheureusement pour l'instant pas possible d'exécuter du code côté serveur sur un site hébergé sur le réseau ZeroNet. Cela n'est pas possible car il n'existe tout simplement pas de serveur sur lequel le code pourrait s'exécuter car le site est partagé entre plusieurs utilisateurs.

Il est toutefois possible de créer des comptes et de se connecter à ces derniers. Les informations de ces comptes sont stockées dans des bases de données MySQL qui sont elles aussi distribuées entre plusieurs utilisateurs grâce au P2P.

ZeroNet permet par exemple d'héberger des sites qui permettent de faire de la discussion instantanée ou encore des forums en tout genre.

Ce réseau est très intéressant pour plusieurs raisons. La première, c'est qu'il ne génère aucun coût d'hébergement car votre site est proposé autant par vous que par tous les autres utilisateurs du réseau qui y ont accédé.

[29] https://www.icann.org/fr

La deuxième raison, c'est qu'il n'y a aucun point unique de défaillance. Dans le cas d'un site web classique, si le serveur qui héberge les différentes pages rencontre un problème, le site n'est plus accessible. Ce n'est ici pas le cas car tant qu'un point d'accès du site existe sur le réseau, le site sera accessible. Le réseau fonctionne sans serveur central et cela représente sa principale force.

Pour terminer avec une troisième raison, les sites hébergés sur ZeroNet ne sont pas censurables. Personne ne peut empêcher l'accès à un site et cela est très important afin de s'assurer que des informations à caractère sensible soient toujours disponibles. Cela permet de s'assurer d'avoir un web libre ou la liberté d'expression et la démocratie sont respectés.

Comme le site du projet le dit si bien, un site est incensurable car il n'est nulle part. Au contraire, il est partout.

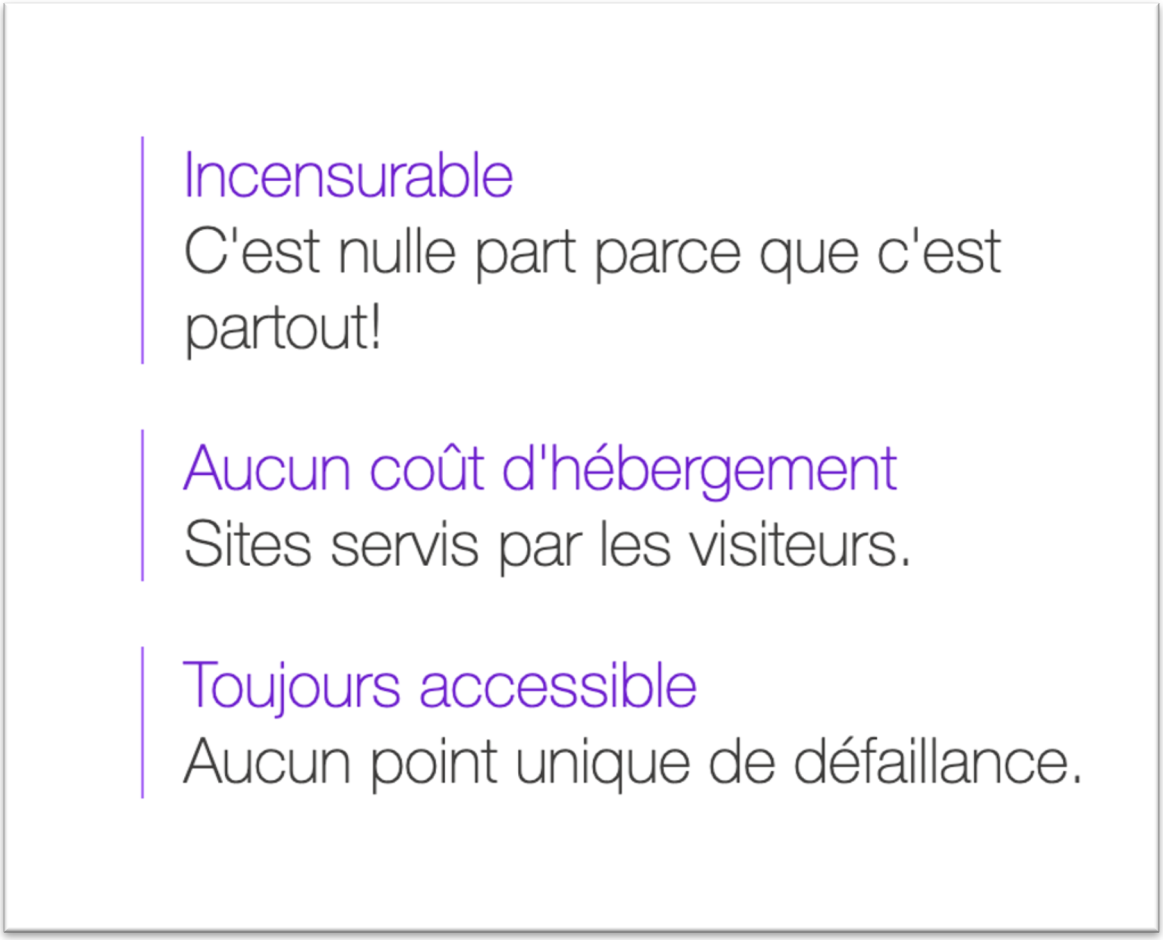

Figure 6 : Points forts de ZeroNet

3.1.2.2 Freenet

Freenet est un autre très bon exemple de ce qu'il est possible d'accomplir en se basant sur les principes du P2P. C'est en Mars 2000 que Ian Clarke publie la première version de son réseau décentralisé. Sa création a été motivée par sa peur de voir disparaître les libertés sur le web, notamment la liberté de la presse.

De ses craintes est né le logiciel Freenet qui est libre et que n'importe qui peut installer sur son ordinateur. Le réseau permet de partager des fichiers ou encore de discuter sur des forums sans craindre la moindre censure et le moindre contrôle sur le contenu ainsi que les idées qui sont partagées.

C'est également via se logiciel qu'il est possible de consulter et de publier ce que l'on appelle des « sitesFree ». Ces sites sont uniquement accessibles via le réseau Freenet et ne peuvent pas être consultés d'une autre manière.

Ce sont les utilisateurs du réseau qui contribuent à ce que ces sites soient accessibles. En effet, chaque utilisateur donne de la bande passante et une petite partie de leur espace de stockage afin de stocker des fichiers appartenant au réseau. Un système automatique choisit quels fichiers sont conservés et lesquels sont supprimés sur les machines des utilisateurs. L'algorithme qui gère ce système se base sur la popularité d'un fichier ou alors sa date de création.

Il est important de noter que les fichiers qui sont stockés sur les ordinateurs des utilisateurs sont chiffrés et ne peuvent donc pas être lus localement. En clair, il est impossible de savoir ce que l'on stocke sur son ordinateur qui appartient au réseau Freenet.

Ce processus est intéressant d'un point de vue sécuritaire car les données des sites que l'utilisateur récupère ne sont pas exploitables. C'est également une bonne chose légalement car vous ne pouvez pas être tenu responsable d'héberger du contenu alors que vous n'avez aucun moyen de savoir ce que ce contenu est réellement.

Freenet est également un réseau qui fonctionne avec des nœuds qui sont mis à disposition par les utilisateurs. Tous les échanges sur le réseau sont chiffrés et passent par plusieurs nœuds afin qu'il soit extrêmement difficile de déterminer d'où vient l'information, quelle est sa destination et enfin, quel est le contenu du message que le réseau transporte.

Il est possible d'utiliser le réseau Freenet via plusieurs autres applications qui s'y connectent afin d'assurer des échanges sécurisés et anonymes. On peut notamment citer Frost qui est un logiciel qui permet de s'échanger des fichiers pair à pair et de pratiquer de la messagerie instantanée sur des boards.

Les boards, que l'on pourrait traduire par forums en français, représentent des espaces qui traitent de sujets divers et variés. Lors du premier lancement de l'application, l'utilisateur n'aura accès qu'à un petit nombre de boards mais sa liste va s'agrandir au fur et à mesure grâce à des mises à jour qui sont publiées régulièrement et qui contiennent une liste des différents boards disponibles. Il est également possible de rechercher des fichiers et de télécharger ces derniers sur son ordinateur grâce à une fonction de recherche intégrée.

Une deuxième application très utilisée est Freemail et comme son nom le laisse présager, cette application permet d'envoyer des emails. Ces emails sont entièrement anonymes et chiffrés car ils transitent via le réseau proposé par Freenet. Le projet est fonctionnel mais a besoin de main d'œuvre afin de continuer à évoluer, le développeur original manquant de temps et ne pouvant pas seul proposer un produit de qualité.

Il existe bien sûr encore d'autres applications qui sont utilisables via le réseau Freenet et un grand nombre sont aujourd'hui encore développées par la communauté sous la forme d'application de bureau ou alors de plug-in pour un navigateur.

Une nouvelle fonctionnalité qui s'intitule « réseau invisible » est venue s'ajouter à Freenet récemment et son idée est très prometteuse. Grâce à une sélection manuelle des nœuds que l'on considère comme sûrs, il est alors possible de créer un réseau basé sur la confiance mutuelle. Un nœud sûr peut par exemple appartenir à un ami ou à une personne de confiance autre. Un réseau se créée ensuite entre ces personnes de confiance et les informations ne sont échangées qu'entre ces différents nœuds. Cela créé donc un réseau dans le réseau qui est totalement imperméable et qui reste sécurisé et anonyme en son sein.

En se connectant ensuite aux amis de ses amis, il est possible d'établir un réseau d'une grande taille entièrement basé sur une confiance mutuelle entre tous les participants. De cette manière, les utilisateurs qui participent à ce « réseau invisible » réduisent leur vulnérabilité mais profitent tout de même d'un réseau d'une grandeur convenable.

Cette façon de faire permet également de créer des accès à Freenet dans des lieux où l'utilisation du logiciel est illégale sans que cela soit possible d'être détecté par un quelconque gouvernement. La censure des gouvernements est donc rendue quasiment impossible car ces « réseaux invisibles » n'ont pas d'accès vers l'extérieur et sont donc impénétrables pour toute personne qui ne s'y trouve pas.

Depuis sa création en 2000, Freenet a été téléchargé plus de 2 millions de fois, ce qui représente une grande réussite pour un projet de ce genre[30]. Il a été utilisé pour la diffusion d'informations que certains gouvernements souhaiteraient censurer, notamment la Chine ou encore certains pays du Moyen-Orient.

Le projet est également très apprécié du milieu universitaire car les idées sur lesquelles il se repose sont des idées qui plaisent et qui sont de plus en plus développées et recherchées.

Dans leurs conceptions ainsi que leurs utilisations, Freenet et ZeroNet sont semblables et proposent les mêmes avantages. Tous les deux permettent d'héberger des sites qui sont uniquement accessibles via leur propre réseau et proposent des services qui garantissent la sécurité et l'anonymat.

La principale différence concerne ce que chaque participant stocke sur son ordinateur. Dans le cas de ZeroNet, il est possible de savoir et de décider ce que l'on souhaite héberger comme contenu sur notre machine. En effet, un site est automatiquement téléchargé puis partagé depuis notre ordinateur lors de notre visite mais rien ne nous oblige à conserver ces données.

Dans le cas de Freenet, il est impossible de savoir quelles sont les données qui sont conservées sur notre ordinateur car elles sont chiffrées. Impossible également de ne pas héberger un certain contenu car il n'est pas possible de manuellement choisir ce que l'on héberge ou non. C'est en effet un algorithme qui va se charger de choisir quels fichiers il faut conserver et lesquels ne sont plus nécessaires. Comme déjà expliqué, cet algorithme se base sur la popularité des fichiers ainsi que sur leurs âges.

Malgré cette différence, les deux réseaux ont les mêmes idées et partagent les mêmes principes. Cela fait d'eux des solutions très intéressantes et utilisables facilement afin de partager du contenu sans être censuré et sans devoir se reposer sur une confiance en une entreprise donc personne ne connaît réellement les intentions et l'utilisation de nos données.

[30] https://www.lesnumeriques.com/telecharger/freenet-23830

3.1.3 Tor

Tor est un réseau décentralisé, disponible partout à travers le monde, construit sur l'infrastructure existante d'internet. Les relais qui composent le réseau sont appelés des nœuds. La liste de ces derniers est publique.

Le but de ce réseau est d'anonymiser tous les échanges de paquets TCP/IP. Le but est qu'il soit impossible de savoir d'où vient le paquet ou quelle est sa destination finale.

Pour anonymiser les échanges de paquets entre un point A et B, les paquets transitent entre plusieurs nœuds qui sont choisis aléatoirement afin de former un circuit. Ce circuit va changer à intervalle de temps régulier afin de rendre le tout plus sécurisé.

La destination des paquets qui sont émis par A sont par exemple R1 (relais 1). Le R1 connaît donc l'adresse IP d'origine mais cela sera le seul dans ce cas. Pour acheminer le paquet plus loin dans le réseau, R1 va l'envoyer à R2, prochain relais sur le circuit prédéfini avant l'envoi. Le paquet a comme source R1 et comme destination R2, il est donc impossible de récupérer à ce moment-là l'adresse IP de A. Ensuite le circuit suit son cours de relais en relais jusqu'à ce qu'un RX (relais x, x représentant le nombre de relais que le paquet a parcouru) achemine finalement le paquet jusqu'à B.

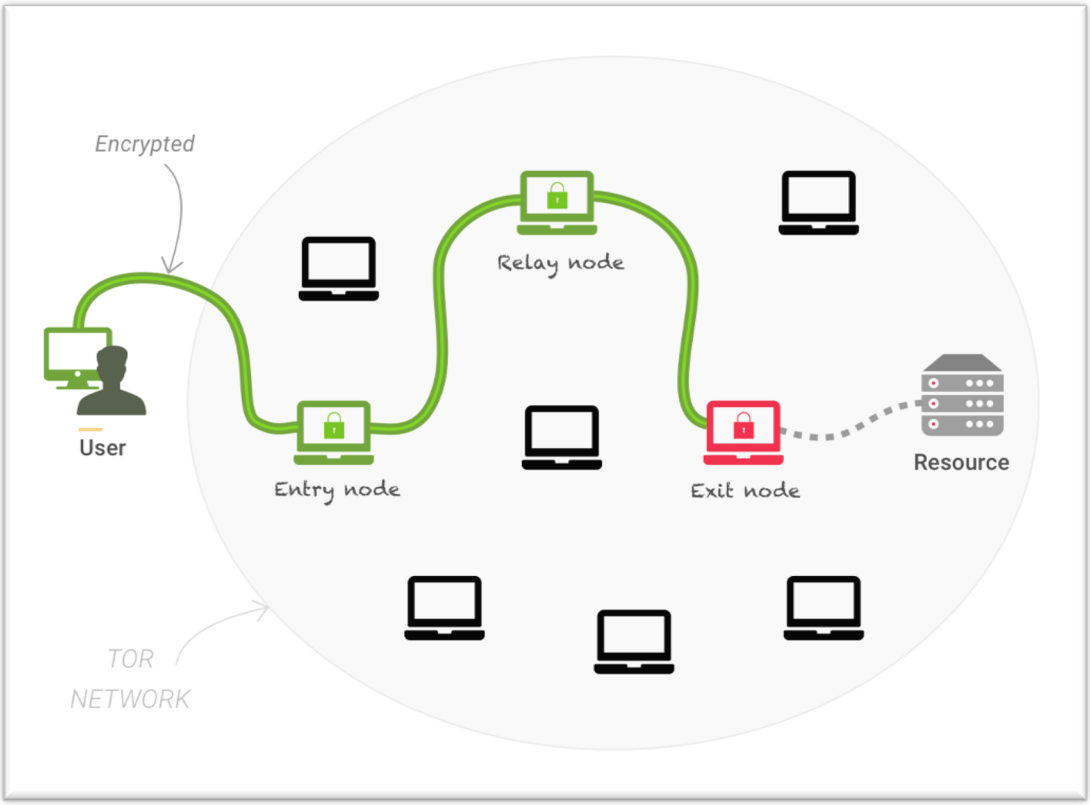

Figure 7 : Exemple de circuit dans le réseau Tor

Source : https://net-security.fr/wp-content/uploads/tor_3.png

Sans rentrer dans les détails cryptographiques des échanges de paquets, il existe un processus assez simple afin que chaque nœud ne connaisse les adresses que de son prédécesseur et de son successeur dans le circuit mais pas de tous les autres nœuds.

Lors de la création du circuit, une clé privée est envoyée à chaque nœud. Cette clé a été chiffrée avec une clé publique qui représente chaque nœud. Après la création du circuit, chaque nœud dispose donc d'une clé privée qui lui est propre et il ne connaît que le nœud d'avant et le nœud d'après.

Avant de partir pour passer d'un nœud à l'autre, le paquet qui part du client va être chiffré un certain nombre de fois. Afin de simplifier, imaginons que notre circuit se compose de 5 appareils :

- Client A (A)
- Nœud 1 (N1)
- Nœud 2 (N2)
- Nœud 3 (N3)
- Client B (B)

Le but est d'envoyer un paquet de A à B et que B puisse bien sûr lire le contenu de ce paquet. L'ordre des nœuds sera N1, N2, N3 puis le nœud final, B.

Sur la machine A, le paquet va donc devoir être chiffré 4 fois. La première fois, le paquet est chiffré avec la clé publique de B, le dernier nœud du circuit.

Le résultat de ce chiffrage est ensuite lui-même chiffré avec la clé publique de N3 puis ensuite celle de N2. Enfin, ce nouveau résultat est lui-aussi chiffré avec la clé publique de N1. Le paquet peut ensuite être envoyé.

Lorsque N1, premier nœud du circuit, reçoit le paquet, il va utiliser sa propre clé privée afin de déchiffrer le paquet. Il va ensuite envoyer le résultat de ce déchiffrement à N2 qui va lui-même déchiffrer le paquet avec sa propre clé privée. Puis, N2 envoie le résultat de son déchiffrement à N3 qui va lui aussi utiliser sa propre clé privée. Pour terminer, le paquet va être transmis à B qui va utiliser sa clé privée afin de retrouver le paquet dans son état original.

Cette façon de faire peut être imagée comme les couches d'un oignon que l'on pèle et c'est pour cette raison que cette façon de faire s'appelle *The Onion Router* que l'on peut traduire par routage en oignon.

L'unique problème réside dans le fait que ce chiffrement / déchiffrement constant ralenti considérablement la vitesse des connexions. Peu importe la bande passante de l'utilisateur, une demande sur le réseau Tor prend considérablement plus de temps qu'une demande classique.

Malgré le fait que les communications à l'intérieur du réseau Tor sont totalement anonymes, les applications que l'on utilise peuvent dans certains cas transmettre des informations annexes qui permettraient de savoir qui est à l'origine ou à la destination.

Afin de palier à ce problème, la fondation qui s'occupe du réseau Tor propose également un navigateur qui s'intitule *Tor Browser*. Ce navigateur est basé sur Firefox et il embarque deux extensions qui garantissent l'anonymat sur le web.

La première extension, *NoScript*, permet de bloquer l'exécution des scripts JavaScript, Flash ou encore d'autres plugins que les sites souhaitent exécuter. Ce blocage est mis en place car les langages de scripting qui s'exécutent dans le navigateur peuvent trahir vos informations personnelles. Des failles dans ces langages sont également régulièrement découvertes et il est donc important d'empêcher l'exécution des scripts afin de s'assurer de notre sécurité.

La deuxième extension s'appelle HTTPS Everywhere et force l'utilisation du HTTPS sur les différents sites web que l'utilisateur consulte. HTTPS rajoute en effet une couche de sécurité supplémentaire entre le client et le serveur qui n'est pas négligeable.

Grâce à ces deux extensions et à l'utilisation du réseau Tor, il est possible de naviguer le web de manière totalement anonyme.

Tor permet également d'accéder à des sites dont le nom de domaine est .onion. Ce nom de domaine est complètement inaccessible depuis les DNS classiques.

Lorsque l'on met en place un service .onion sur un serveur connecté au réseau Tor, les utilisateurs qui souhaitent accéder à ce service n'accèderons jamais réellement au serveur. Lorsqu'un client fait une demande pour accéder à un contenu hébergé sur un serveur .onion, le système va organiser un rendez-vous sur un nœud dans le réseau Tor au lieu de simplement fournir l'adresse IP du serveur.

Cela permet d'échanger les paquets voulus sans que le client connaisse l'adresse du serveur et vice-versa. Cela rend le client et le serveur bien plus difficile à tracer, autant l'un par rapport à l'autre que pour d'éventuels intermédiaires qui tenteraient de surveiller le trafic.

C'est pour cette raison que les services qui sont accessibles via une adresse en .onion sont appelés des services cachés. A noter qu'on ne peut pas choisir une adresse .onion, elle sera définie par la clé publique émise lors de la configuration du service sur le réseau.

A titre d'exemple, l'adresse actuelle de Facebook sur le réseau Tor est la suivante :

https://www.facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion/

Certains sites, notamment Facebook, proposent une version de leurs services via le réseau Tor car ces services seront accessibles depuis des pays ou ces sites sont normalement inaccessibles car censurés par le gouvernement.

Bien que Tor permette un anonymat intéressant sur le web, la conception de son réseau ne propose pas des services qui soient décentralisés. Certes il sera extrêmement délicat pour un acteur externe de faire fermer un site .onion mais cela n'est pas impossible.

C'est notamment ce qui est arrivé au site Silk Road qui était spécialisé dans la vente de produits illicites. Le FBI a réussi à faire fermer deux fois le service, la première fois en 2013 puis une seconde fois en 2014[31].

Cela a été possible car l'hébergement des sites .onion n'est pas décentralisé, toutes les informations sont toujours contenues sur un serveur en particulier. L'accès est décentralisé car il se fait toujours sur un autre nœud du réseau mais cette centralisation de l'information provoque l'apparition d'un point de défaillance unique qui peut être exploité afin de censurer un service en particulier.

En conclusion, Tor représente donc une excellente alternative pour se protéger de la traque incessante de nos activités sur Internet mais ne propose pas une réelle décentralisation des ressources qui permet de s'assurer que ces dernières soient toujours accessibles et non censurables.

[31] https://fr.wikipedia.org/wiki/Silk_road

3.2 Avantages d'un web décentralisé

Après avoir passé en revue plusieurs solutions qui permettent une décentralisation du web, nous allons maintenant nous intéresser aux avantages qu'une telle décentralisation peut apporter aux utilisateurs.

Afin de classer ces avantages en plusieurs catégories, les points suivants seront abordés. Il s'agira tout d'abord de comprendre en quoi cela impacte les services que nous utilisons tous les jours et si ces types de services peuvent être mis en place via ces solutions. Si c'est le cas, il sera intéressant de comprendre qui mettrait à disposition ces services et comment ces derniers seraient exploités.

Il s'agira ensuite de s'intéresser au nerf de la guerre, à savoir toutes nos données personnelles que nous partageons sur le web. Nous allons tenter de comprendre en quoi une décentralisation change la donne pour nos données.

Nous parlerons également de l'infrastructure que ces solutions nécessitent afin de fonctionner convenablement et quelles sont les différences majeures entre ce genre de solutions et le web classique que nous connaissons aujourd'hui.

Pour terminer, nous passerons en revue l'impact environnemental de ces solutions ainsi que les répercussions majeures que ces dernières pourraient avoir sur la société telle que nous la connaissons actuellement.

3.2.1 Les services

Durant la première partie de ce travail, il a beaucoup été question des services qui sont mis à disposition par les géants du web. Ces services, qui sont utilisés par plusieurs millions voire plusieurs milliards de personnes, sont imaginés, construits puis ensuite exploités par ces entreprises qui tiennent le web d'une main ferme. Nous avons pu nous rendre compte que le principal problème réside justement dans le principe qu'ils peuvent faire ce qu'ils veulent avec leurs services et nous, clients, sommes obligés d'accepter les changements ou alors même la suppression pure et dure d'un service. Nous devons également accepter des conditions d'utilisations souvent peu claires sous peine de se voir refuser l'accès au service.

Le paragraphe précédent représente la situation actuelle du web centralisé que nous utilisons tous les jours mais est-ce que des services équivalents pourraient exister dans un web complètement décentralisé comme ZeroNet ou Freenet ?

Pour qu'un service fonctionne, il faut que ce dernier ait été correctement imaginé et développé. Pour ces tâches, il sera toujours nécessaire qu'un développeur individuel ou alors une entreprise se charge de la conception et du développement du produit.

Cependant, il est déjà possible d'émettre une différence lorsque le développement du service est terminé. Il sera très important que le code qui compose ce service soit open source. Cela signifie que n'importe quelle personne le souhaitant peut consulter le code source complet de l'application et donc savoir précisément ce qu'il s'y passe. Ce n'est bien sûr pas le cas des services mis à disposition par les géants du web. Ces derniers ne sont pas open source et il est donc impossible pour qui que ce soit de savoir précisément ce qu'il se trame dans le fonctionnement de l'application.

Une fois un service prêt à être exploité, il faut le mettre à disposition des utilisateurs afin que ces derniers puissent l'utiliser comme ils le souhaitent. Dans le cas d'un web décentralisé, cela veut dire mettre le service à disposition sur sa propre machine puis ensuite attendre que d'autres utilisateurs s'y connectent afin qu'ils récupèrent le site sur leurs machines puis soient ensuite source pour les utilisateurs suivants.

De cette manière, le service va rapidement se propager sur le réseau afin d'être accessible en tout temps et de gagner en rapidité. Dans cette manière de faire, une différence particulièrement intéressante saute aux yeux.

Les services des GAFA ne se propagent pas sur le web, ils sont hébergés sur des serveurs appartenant à l'entreprise et les clients viennent récupérer les données sur ces serveurs. Dans le cas de la décentralisation, tous les clients qui se sont un jour connectés au service vont désormais faire office de serveur pour les prochains.

Cela veut donc dire que les GAFA ont la possibilité, s'ils le souhaitent, de complètement arrêter un service du jour au lendemain. Pour se faire, il leur suffit de mettre hors ligne les serveurs qui contiennent le code de ces services. Dans un web décentralisé, cela est impossible, personne ne possède un tel contrôle, pas même le créateur originel du service.

Une fois que le service s'est propagé, il est impossible de l'arrêter. Tant qu'une personne qui a visité le service garde son ordinateur allumé, ce dernier agira comme serveur et donc le service existera toujours. Cela apporte plusieurs avantages. Tout d'abord, le créateur, c'est-à-dire le développeur ou alors l'entreprise créatrice du service, n'a pas la mainmise sur le service. Ce dernier vit à travers tous les utilisateurs et ne peut pas être mis hors ligne par ses créateurs.

Cela est notamment très intéressant d'un point de vue de la censure. Si un gouvernement souhaite rendre inaccessible un service sur son territoire, cela ne sera pas possible en raison de la propagation de ce dernier sur le réseau décentralisé.

Les créateurs originels perdent donc le pouvoir sur leur service mais cela ne les empêche pas d'ajouter de nouvelles fonctionnalités. En effet, ils possèdent une clé unique et privée qui va permettre de signer une modification du code du service en attestant qu'il a été produit par les créateurs du service. Ce nouveau code sera ensuite propagé sur le réseau aux clients afin que la nouvelle version soit accessible depuis toutes les sources.

En résumé, l'utilisation des services ne diffère pas par rapport au web actuel mais la grande différence réside dans le contrôle réduit au minimum de la part des créateurs sur leurs produits. De cette manière, la confiance envers le produit est plus grande car bien qu'il ait été créé par une personne en particulier, le code est entièrement disponible et le contrôle total est retiré des mains des créateurs afin de le déposer dans les mains de milliers d'utilisateurs.

En conclusion, le web décentralisé est tout à fait à même de proposer des services aux utilisateurs aussi performants et riches en fonctionnalités que ceux que nous connaissons sur le web actuellement tout en garantissant que ces services ne soient pas contrôlés par une entreprise ou censurés par un gouvernement.

3.2.2 Les données

Dans le premier chapitre de ce travail, nous avons pu nous apercevoir que les données que nous déposons sur les services des géants du web représentent une mine d'or pour ces derniers. C'est en effet grâce à nos données que la majorité de leurs revenus sont générés chaque année. Comme nous avons pu le voir dans les conditions d'utilisations de ces services, les données que nous y déposons ne nous appartiennent plus et ces entreprises peuvent en faire ce qu'elles en veulent car nous leur en donnons le droit.

Dans le cas d'un web décentralisé, cela se passe différemment. Lors de l'utilisation d'un service décentralisé, vous ne fournissez jamais vos données à un serveur distant dont vous ne savez ni l'emplacement, ni ce dernier est correctement sécurisé ou encore ce qu'il adviendra réellement de vos données. Lorsque vous vous connectez à un service, vos données seront certes partagées avec d'autres utilisateurs source de ce service mais elles ne seront jamais stockées sur un serveur central et surtout jamais utilisées à des fins publicitaires notamment.

C'est l'utilisateur qui garde le contrôle de ses propres données et il peut s'il le souhaite, supprimer complètement ses données du réseau décentralisé et les copies qui peuvent exister sur d'autres appareils appartenant au réseau seront également détruites. De cette manière, nous partageons tout de même des données avec d'autres utilisateurs mais nous restons le maître de ces données et nous pouvons décider ce que nous souhaitons en faire.

Cela représente l'un des principaux arguments d'une décentralisation du web car l'utilisation de nos données personnelles est l'un des plus gros problèmes du web actuel.

Qu'elles soient utilisées à des fins publicitaires ou alors encore revendues afin d'établir des statistiques ou d'influencer des élections politiques, nous en perdons totalement le contrôle et cela fait, à raison, de plus en plus peur aux utilisateurs. Les fuites de données représentent également un gros problème et une centralisation de gigantesques bases de données facilitent la vie des pirates qui cherchent à acquérir ces informations.

Dans un web décentralisé, nous n'avons pas besoin de faire confiance aveuglement à de grandes entreprises et nous pouvons décider quelles données sont stockées sur le réseau. La sécurité est également renforcée car il est plus bien plus difficile de s'emparer de données éparpillées à plusieurs centaines d'endroits sur un réseau plutôt que dans un serveur unique dans un centre de données.

3.2.3 L'infrastructure

En l'état actuel, le web a besoin d'une infrastructure gigantesque afin de pouvoir fonctionner correctement. Au-delà des nombreux câbles et équipement réseaux qui sont disposés partout à travers le globe, il a fallu trouver une solution afin de stocker des quantités astronomiques de données et de fournir de la puissance de calcul pour les services qui en ont besoin.

Pour pallier à ce problème, d'imposants centres de données ont été construits à travers le monde et une quantité impressionnante de projets sont en consultation car le web continue de grandir et les demandes en matériel vont continuer d'augmenter. C'est justement la centralisation du web qui oblige les fournisseurs de services d'acquérir ou de louer du matériel leur offrant de la puissance de calcul et un espace de stockage permettant de conserver les données nécessaires.

Sans les centres de données, le web ne fonctionnerait tout simplement pas. A titre d'exemple, Google a fait construire pas moins de 21 centres de données à travers le monde afin de pouvoir mettre à disposition leurs services de manière performante.

Cette infrastructure gigantesque pose plusieurs problèmes et l'un d'eux est le coût faramineux que ces centres de données nécessitent, autant durant leur conception que leur construction ou encore leur exploitation. En 2019, Google a par exemple investi pas moins de 13 milliards de dollars pour leur infrastructure physique[32].

Une centralisation du web représente donc des coûts énormes, autant pour les exploitants de ces centres de données que pour les potentiels clients qui souhaitent héberger leurs services. Cela sans compter sur le fait que cette infrastructure doit être maintenue en état d'utilisation et souvent remplacée afin d'évoluer avec les standards techniques qui changent continuellement.

Dans une certaine mesure, une décentralisation du web résoudrait ce problème car un partage des données des sites entre tous les utilisateurs ne nécessite pas l'utilisation d'un centre de données. Nul doute que pour certains services coûteux en puissance ou alors en espace de stockage, les ordinateurs de tous les utilisateurs ne suffiraient pas. Il faudrait alors que plusieurs de ces utilisateurs investissent dans des équipements plus coûteux afin que le service reste performant. Même en utilisant cette solution intermédiaire, les centre de données ne sont pas nécessaires et ce sont de grandes économies que les fournisseurs ainsi que les clients pourraient réaliser.

[32] https://www.cnbc.com/2019/02/13/google-will-spend-13-billion-on-real-estate-moves-in-2019.html

3.2.4 L'environnement

Le second et sûrement le plus gros problème de l'infrastructure actuelle qui permet au web de fonctionner, c'est l'impact environnemental. Dans un monde où les préoccupations liées au dérèglement climatique sont de plus en plus présentes, comment continuer à exploiter une infrastructure extrêmement énergivore et polluante alors que des solutions plus vertes sont à portée de main.

Le principal problème réside dans la consommation excessive d'électricité. En effet, il faut tout d'abord fournir en électricité tous les serveurs et équipement réseaux qui composent le centre de données. Malheureusement, ces équipements produisent énormément de chaleur et il faut donc refroidir le bâtiment pour que les équipements continuent à fonctionner normalement et répondent aux attentes en termes de performance. Pour refroidir le bâtiment, plusieurs solutions sont possibles et la plupart sont très énergivores.

Selon une étude parue en 2013, un centre de données de 10'000 m2 consomme autant qu'une ville de 50'000 habitants[33], ce qui représente une énorme quantité d'énergie.

L'exploitation des centres de données à travers le globe sont également responsables de 0.3% des émissions mondiales de gaz à effet de serre qui ont un impact grave sur le climat de notre planète[34].

En passant à un web décentralisé, la notion de clients et serveurs disparait complètement pour laisser la place à un réseau où tous les acteurs occupent les deux rôles. En utilisant le matériel de tous les utilisateurs disponibles à travers le monde, il est envisageable de proposer un réseau avec les mêmes performances que le web actuel.

Tout cela en économisant beaucoup d'énergie car le besoin en centres de données sera grandement réduit, les données étant hébergées chez les différents utilisateurs du réseau, sans coût supplémentaire pour refroidir ou alimenter de gigantesques bâtiments abritant des milliers d'appareils informatique.

[33] https://www.batiactu.com/edito/quand-l-informatique-sert-aussi-a-se-chauffer-35613.php
[34] https://www.nature.com/articles/d41586-018-06610-y

3.2.5 L’aspect social

L’aspect social d’un web décentralisé serait bien sûr très important car cela modifierait en profondeur la mainmise des gouvernements et des grandes entreprises sur les informations qui s’échangent via un réseau mondial interconnecté.

Nous avons pu nous apercevoir que la censure des informations ainsi que la surveillance sont omniprésentes sur le web actuel car sa structure facilite grandement ce genre de pratiques.

Avec le passage à un web décentralisé, ces pratiques ne seraient plus possibles. Comme nous l’avons vu lors du chapitre présentant les solutions techniques, ces dernières ne permettent pas de remonter jusqu’à la source de l’information première ou encore de bloquer un site de manière arbitraire.

La censure est rendue impossible par le fait que les sites sont hébergés et partagés par un grand nombre d’utilisateurs du réseau, il n’est donc plus possible de bloquer le serveur central afin de s’assurer que les informations ne soient pas accessibles.

La surveillance est également rendue quasiment impossible car les réseaux sont constitués d’un grand nombre de nœuds qui permettent de faire rebondir les connexions plusieurs fois de la source à la destination. De cette manière, il est impossible pour un tiers de savoir d’où vient le paquet intercepté et quelle est sa destination. L’anonymat est donc assuré.

Cette technique de nœuds permet également d’accéder à du contenu qui serait bloqué de manière géographique par un certain gouvernement. En effet, comme les connexions sont anonymes, une connexion au réseau décentralisée est le seul prérequis afin de pouvoir accéder à l’entièreté de son contenu, peu importe l’endroit où l’on se trouve.

Pour conclure, un web décentralisé permettrait vraiment d’offrir à tout un chacun un espace de liberté total où la démocratie, la liberté d’expression ainsi que la liberté de la presse sont les maîtres mots. Cela n’est malheureusement pas le cas sur le web actuel et cela doit changer afin que n’importe qui puisse accéder à de l’information de qualité ou encore exprimer ses opinions de manière libre, sans craindre la censure ou des répercussions.

3.3 Dérives d'un web décentralisé

Il est bien sûr impossible d'offrir une solution qui se compose uniquement de points positifs, c'est pourquoi les dérives potentielles d'un web décentralisé sont également abordées.

Si l'on ne s'intéresse qu'aux bons côtés, une liberté totale semble être le paradis en termes de démocratie, liberté de la presse ou encore liberté d'expression. Cependant, bien qu'une grande majorité des personnes soient bien attentionnées, il est malheureusement impossible de freiner les personnes dont les intentions sont plus sombres.

La liberté étant totale et la censure impossible, n'importe qui peut publier des pages ou encore des forums sur le sujet qu'il souhaite avec le contenu qu'il souhaite. Il est donc fort probable qu'un web décentralisé se retrouve rapidement infesté de sites contraires aux bonnes mœurs.

Au-delà de sites au contenu réprimable, il est également possible de voir apparaitre des sites sur lesquels il est possible de se procurer du matériel illégal, par exemple des armes ou encore de la drogue. Cela est un phénomène déjà présent sur le réseau Tor qui contient des sites qui vendent des produits illégaux. Certains gouvernements, notamment les États-Unis, se battent continuellement afin de faire fermer ces sites mais la structure de Tor rend difficile la censure. Cela peut donc prendre plusieurs mois ou même années mais quelques sites ont pu être fermés.

Pour se rendre compte des dérives d'un système décentralisé en utilisant un exemple qui existe déjà, on peut parler du Bitcoin. La première crypto-monnaie qui a révolutionné la façon d'entreprendre l'économie est aujourd'hui utilisée par une majorité d'activité légales mais aussi par quelques activités plus louches.

La structure d'une chaine de blocs ne permettant pas de savoir à qui on envoie réellement de l'argent, certains pirates s'en servent afin de collecter des rançons. Ces rançons sont demandées à la suite de l'infection d'un ordinateur par ce que l'on appelle un ransomware. Ces virus, que l'on attrape souvent à la suite de l'exécution d'un logiciel infecté, chiffrent l'entièreté du disque dur de l'ordinateur avec une clé de chiffrement que seul le pirate possède. Un message vous invitera ensuite à envoyer une certaine quantité de Bitcoin à une certaine adresse afin de récupérer la clé de chiffrement et de pouvoir récupérer l'accès à vos données.

L'anonymat fournit par la chaîne de blocs ne permet ensuite pas de savoir à qui a réellement été envoyé l'argent et il devient donc impossible de mener des enquêtes afin de se débarrasser des créateurs de ces virus qui causent de gros dégâts.

Dans l'exemple si dessous, une fenêtre s'ouvre après le chiffrement des données de l'ordinateur et demande d'envoyer 300$ en Bitcoin.

Figure 8 : WannaCry, un exemple de ransomware[35]

Pour conclure, dans une écrasante majorité des cas, une liberté totale est un atout et sera utilisé de la bonne manière afin de proposer un service ou de faire parvenir une information importante à des gens qui en ont besoin. Mais malheureusement, il est impossible d'empêcher l'utilisation de cette liberté par des personnes mal intentionnées qui pourront sans autre mettre en place ce qu'ils souhaitent.

C'est malheureusement le risque à prendre pour obtenir un web complètement libre. Il s'agit ensuite de se demander jusqu'à où la liberté doit être préservée et si un peu de contrôle n'est pas toujours nécessaire afin de maintenir l'ordre. Cette question complexe pourrait faire l'objet de son propre travail afin de trouver un équilibre assurant liberté mais réprimandes des contenus trop extrêmes.

[35] https://www.usine-digitale.fr/mediatheque/9/6/7/000547769_homePageUne/ransomware-wannacry.jpg

3.4 Intervention des gouvernements

Au-delà d'organisations non-gouvernementales et de certaines personnalités influentes, certains gouvernements se rendent également compte du problème posé par les GAFA et cherchent à réduire et maîtriser leur puissance.

C'est notamment le cas de l'union européenne qui ne souhaite pas bannir ces grandes entreprises mais qui souhaite contenir leur pouvoir. Le plan de l'UE se compose de trois points :

- Des amendes
- Des taxes
- Des lois

Les amendes viennent punir les GAFA lorsque ceux-ci ne respectent pas des lois qui sont en vigueur en Europe. Ces lois sont uniques et ne sont pour la plupart pas présentes sur d'autres espaces géographiques, les entreprises doivent donc s'adapter spécialement pour l'union européenne.

Malgré cela, certaines entreprises ne respectent pas ces lois et se voient infliger des amendes. C'est notamment le cas de Google avec leur produit Android[36].

> *L'Union européenne a infligé mercredi une amende record de 4,34 milliards d'euros à Google pour avoir abusé de la position dominante de son système d'exploitation pour smartphones, Android, afin d'asseoir l'hégémonie de son service de recherche en ligne. – Libération, 18 juillet 2018*

Ce qui est reproché à Google, c'est d'obliger les fabricants de smartphones Android à proposer par défaut la recherche Google à ses clients. De cette manière, l'entreprise s'assure plus d'utilisateurs pour son moteur de recherche car plus de 70% des appareils mobiles dans le monde utilisent Android comme système d'exploitation[37]. L'amende n'a pas encore été payée car Google va contester la décision en justice prochainement.

La deuxième façon de réduire l'influence des géants du web, c'est de mettre en place des taxes qui vont limiter leurs revenus. C'est notamment le cas du gouvernement français qui a mis en place une « taxe sur les services numériques » en juillet 2019[38].

> *La taxe a été fixée à 3% du chiffre d'affaires des entreprises du numérique dont le revenu dépasse les 750 millions d'euros et dont au moins 25 millions sont rattachés à une activité en France. – SiècleDigital, 1er septembre 2021*

[36] https://www.liberation.fr/planete/2018/07/18/android-google-condamne-par-bruxelles-a-43-milliards-d-euros-d-amende_1667423/
[37] https://gs.statcounter.com/os-market-share/mobile/worldwide
[38] https://siecledigital.fr/2021/09/01/la-taxe-gafa-a-rapporte-375-millions-deuros-a-la-france-en-2020/

Ainsi, en 2020, cette taxe a rapporté 375 millions d'euros à l'état français. De cette manière, les revenus des entreprises sont limités et cela limite leurs pouvoirs. La France est le premier pays de l'union européenne à imposer des taxes aussi lourdes mais d'autres pays devraient suivre dans leurs traces prochainement.

Enfin, le troisième axe d'action pour l'UE est la mise en place de nouvelles lois qui vont changer le monde digital en Europe. L'idée est d'appliquer au web le même principe de libre circulation qui s'applique déjà pour les personnes et les marchandises en Europe.

La première de ces nouvelles lois, nommée RGPD (Règlement Général sur la Protection des Données), a vu le jour en mai 2016. Le but premier était d'harmoniser l'ensemble des lois des pays membres afin que protection des données soit appliquée de manière uniforme.

Le texte contient énormément de nouvelles dispositions mais deux sortent du lot afin de protéger les utilisateurs des géants du web. La première concerne le consentement des utilisateurs lors de leur visite sur un site web.

> *Les entreprises et organismes doivent donner aux citoyens davantage de contrôle sur leurs données privées, notamment via l'acceptation des cookies sur les sites internet et sur le contrôle de l'utilisation qui est faite des données que les internautes envoient dans les formulaires de contact. Par exemple, il n'est plus possible que la case « j'accepte de recevoir la newsletter » soit pré-cochée lors de l'envoi d'un formulaire de contact dans lequel l'e-mail est renseigné. – RGPD*

Il est maintenant commun de pouvoir refuser ou accepter l'utilisation des cookies sur un site grâce à cette loi. Ainsi, si l'utilisateur ne souhaite pas utiliser les cookies, il a le droit de refuser et le site doit accepter ce refus et ne stocker aucun cookie.

Le deuxième point intéressant concerne la suppression de données que l'on souhaiterait voir disparaître du web.

> *La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais pour 6 motifs. – RGPD*

Il est ainsi possible de demander à n'importe quel site de supprimer des données nous concernant, ce qui était impossible avant l'apparition de cette nouvelle loi. Cette nouvelle loi et d'autres qui vont suivre ont pour objectif de remettre la vie privée des utilisateurs au centre de l'attention, ce qui représente un pas dans le bon sens.

En Suisse aussi, le gouvernement ne peut ignorer l'emprise des GAFA sur le monde digital et cherche donc à établir une gouvernance numérique capable de protéger sa population au mieux.

Le Conseil Fédéral a défini une stratégie qui s'intitule « Suisse Numérique » et qui pose les lignes directrices que toutes les parties prenantes du numérique en Suisse se doivent de suivre. Cette stratégie s'articule tout d'abord autour de 5 objectifs principaux :

- Établir l'égalité des chances entre tous et renforcer la solidarité
- Garantir la sécurité, la confiance et la transparence
- Renforcer l'autonomie et l'autodétermination numérique des personnes
- Assurer la création de la valeur, la croissance et la prospérité
- Réduire l'empreinte écologique et la consommation d'énergie

Ces objectifs ne ciblent pas directement les GAFA en leur imposant des lois ou taxes comme l'union européenne, mais ils rejoignent l'idée que l'espace numérique doit être plus démocratique et ouvert, notamment en mettant l'accent sur des chances égales et une solidarité renforcée.

Il est aussi intéressant de noter que la sécurité, la confiance et la transparence sont aussi au cœur de la stratégie. Sans le nommer explicitement, cet objectif fait référence à nos données personnelles que nous fournissons aux acteurs du numériques. Ces derniers doivent donc correctement les sécuriser et être transparents sur la façon dont ils les utilisent. De cette manière, les utilisateurs peuvent leur faire confiance.

Enfin, il est intéressant de noter que réduire l'impact sur l'environnement du secteur numérique est également quelque chose que le gouvernement suisse tient à cœur. Comme nous l'avons déjà vu dans ce travail, un web décentralisé peut apporter une solution à cette consommation excessive d'énergie.

Pour arriver à ces objectifs, la stratégie se doit également de respecter 4 principes :

- Placer l'être humain au centre des préoccupations
- Offrir des conditions propices au développement
- Faciliter le changement structurel
- Organiser les processus de transformation au moyen d'une approche en réseau

Avec ces objectifs en tête et des principes à respecter, la Suisse souhaite ainsi inclure tous les habitants du pays dans la transformation numérique et offrir des chances égales à tous.

> *Pour que tous les habitants de la Suisse puissent bénéficier des avantages de la transformation numérique, les autorités de tous les niveaux fédéraux, la société civile, les entreprises, le monde scientifique et les milieux politiques doivent œuvrer ensemble en vue de favoriser le changement. – Stratégie Digitale Suisse*

4. Mise en place d'un site web

Afin de démontrer qu'il n'est pas difficile de rejoindre le mouvement d'un web décentralisé, je vais maintenant expliquer comment n'importe qui peut ajouter un site web d'information sur le réseau ZeroNet.

Tout d'abord, il s'agit d'installer l'application ZeroNet sur son ordinateur. Cette application est téléchargeable via le github officiel du projet[39]. L'application s'installe ensuite normalement comme toute autre application et est disponible sur toutes les plateformes grand public, à savoir Windows, macOS et les distributions Linux.

Une fois l'application installée, il faut lancer celle-ci. En ouvrant l'application, un script python va être lancé sur la machine puis la page d'accueil du projet va nous être proposée dans le navigateur par défaut.

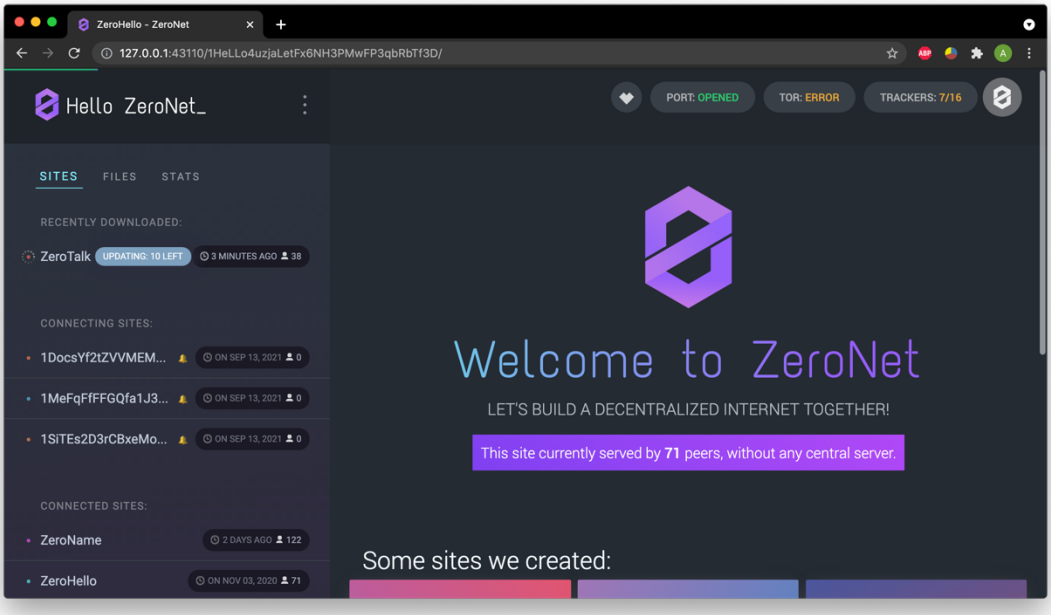

Figure 9 : Page d'accueil de ZeroNet

Cette page d'accueil contient plusieurs informations importantes concernant l'état de santé du réseau.

A gauche, la liste des sites auxquels l'utilisateur est connecté et sert de serveur pour les autres utilisateurs. Ici par exemple, les données de ZeroTalk sont en train d'être mise à jour pour correspondre à la dernière version du site.

[39] https://github.com/HelloZeroNet/ZeroNet#user-content-how-to-join

En haut à droite, plusieurs informations concernant notre connexion au réseau :

- *Port : Opened* permet de s'assurer que le port 15673 nécessaire au bon fonctionnement de ZeroNet est ouvert sur le routeur.
- *Tor : Error* permet de savoir si Tor est utilisé au-dessus de ZeroNet. Cela permet d'assurer un anonymat quasi-total.
- *Trackers : 7/16* nous tient à jour de l'état des trackers utilisés pour le bon fonctionnement du réseau. Dans mon cas, je suis connecté à 7 d'entre eux.

Enfin, sur la partie centrale, le message d'accueil du projet nous explique que le site sur lequel nous naviguons n'est pas hébergé sur un serveur central mais partagé par 71 personnes actuellement.

Sur le bas de la page, des liens redirigent vers les projets les plus emblématiques du réseau afin de pouvoir rapidement se faire une idée de comment ce dernier fonctionne.

Pour créer un nouveau site vide, il faut cliquer sur les 3 petits points qui se situent à côté du titre de la page « Hello ZeroNet » puis choisir « Create new, empty site ».

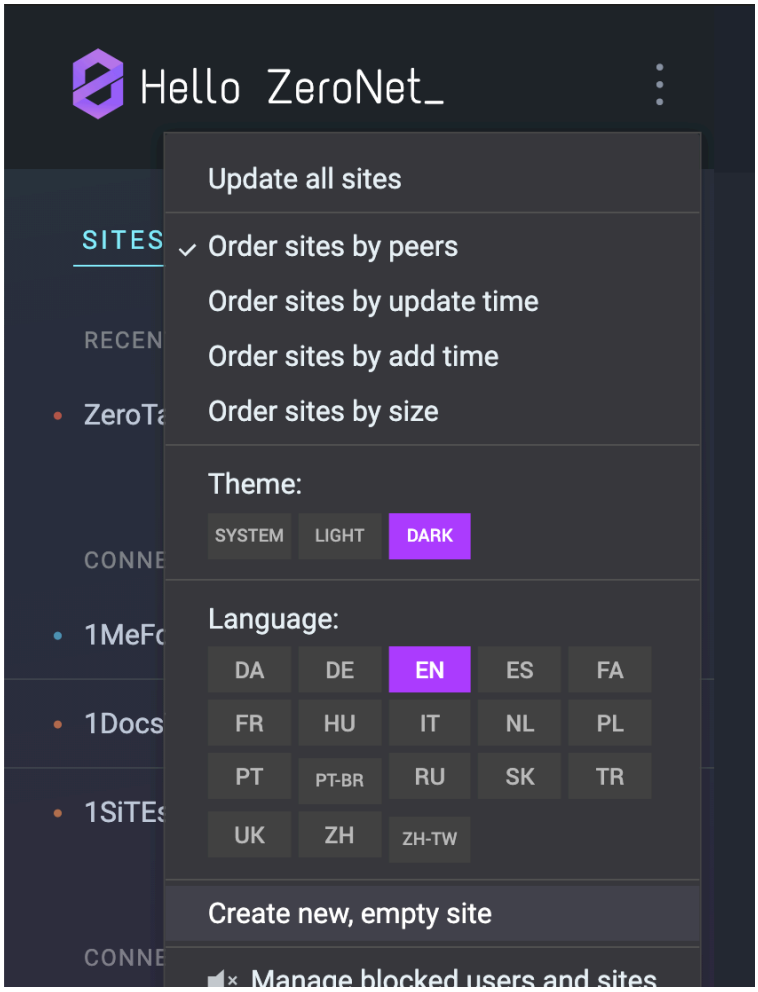

Figure 10 : Menu de ZeroNet

Après avoir cliqué sur ce bouton, notre nouveau site est créé et nous sommes redirigé sur la page de ce site. Plusieurs informations sont alors disponibles.

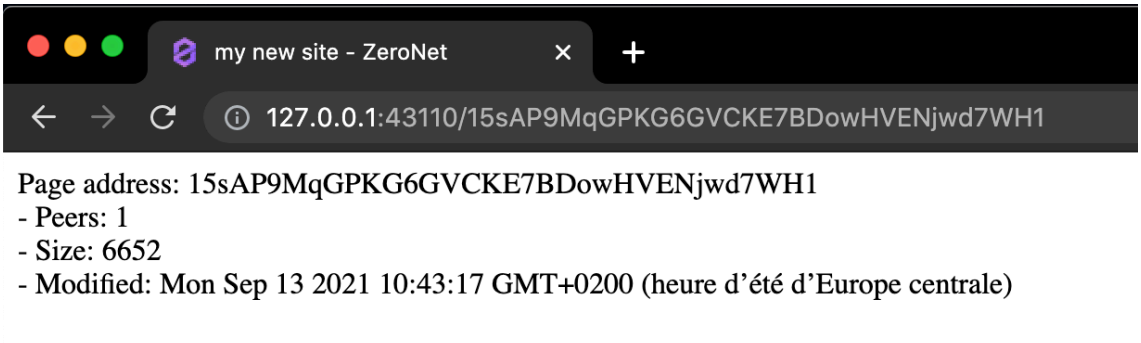

Figure 11 : Exemple de site créé sur ZeroNet

- *Page address*, comme son nom l'indique, représente l'adresse de notre site.
- *Peers* permet de savoir combien de personnes partagent notre site. Pour le moment, un seul car le site vient d'être créé et n'a pas encore été visité par d'autres utilisateurs.
- *Size* permet de savoir quelle taille notre site occupe sur le disque.
- *Modified* permet de savoir à quelle date le site a été modifié pour la dernière fois.

Une fois la création du site terminée, il s'agit maintenant d'ajouter du contenu. Pour se faire, il faut accéder aux fichiers du site qui sont stockés sur l'ordinateur.

Je n'ai pas eu l'occasion de tester ZeroNet sur d'autres systèmes d'exploitation mais sur macOS, le chemin pour accéder aux fichiers de notre site est le suivant.

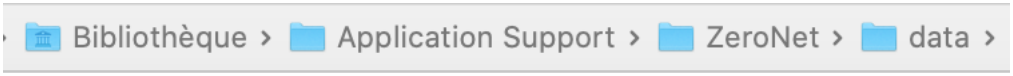

Figure 12 : Chemin des fichiers d'un site ZeroNet

Une fois dans ce dossier, il devrait exister un dossier qui porte le nom de notre site, à savoir la clé publique de ce dernier. Dans ce dossier, 3 éléments sont présents :

- *content.json* est le fichier le plus important du site. C'est lui qui contient toutes les informations nécessaires au bon fonctionnement du site sur le réseau. En règle générale, il n'est pas nécessaire d'y toucher.
- *index.html* est le fichier de base qui est affiché sur notre site. C'est ce dernier que nous allons modifier afin de présenter du contenu aux utilisateurs qui visitent notre site.
- *js* est un dossier qui contiendra les fichiers JavaScript éventuellement nécessaires au bon fonctionnement de notre site.

Afin de renseigner le contenu du site, il faut donc modifier le fichier index.html. Dans ce dernier, il est possible d'utiliser du HTML classique tel qu'on le connaît sur le web actuel.

Une fois que vous êtes satisfait avec le contenu du fichier index.html, il faut sauvegarder celui-ci puis se rendre à nouveau sur la page de notre site.

Après un rafraichissement de la page, le système de ZeroNet va se rendre compte que les fichiers du site ont changés et va donc vous proposer de signer ces changements et de les publier afin qu'ils soient propagés sur le réseau. Une petite fenêtre va apparaître en bas à droite de la page.

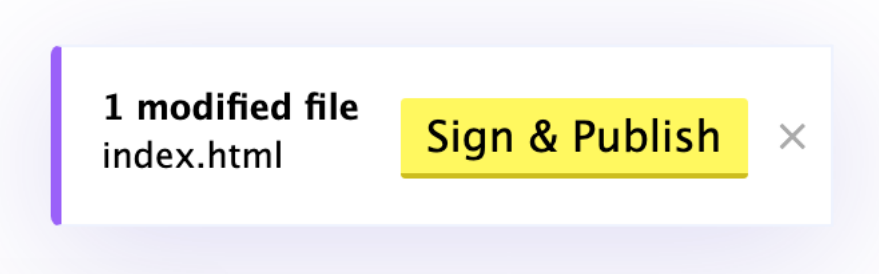

Figure 13 : Signer et publier un site ZeroNet

Si tout se passe correctement, un message de succès devrait s'afficher et le site est maintenant accessible à tous les utilisateurs de ZeroNet via l'adresse publique de ce dernier.

Il est également intéressant de noter que lorsque vous êtes sur votre site, il est possible de tirer le logo ZeroNet (en haut à droite de la page) sur la gauche en restant cliqué afin de faire apparaitre un tableau de bord.

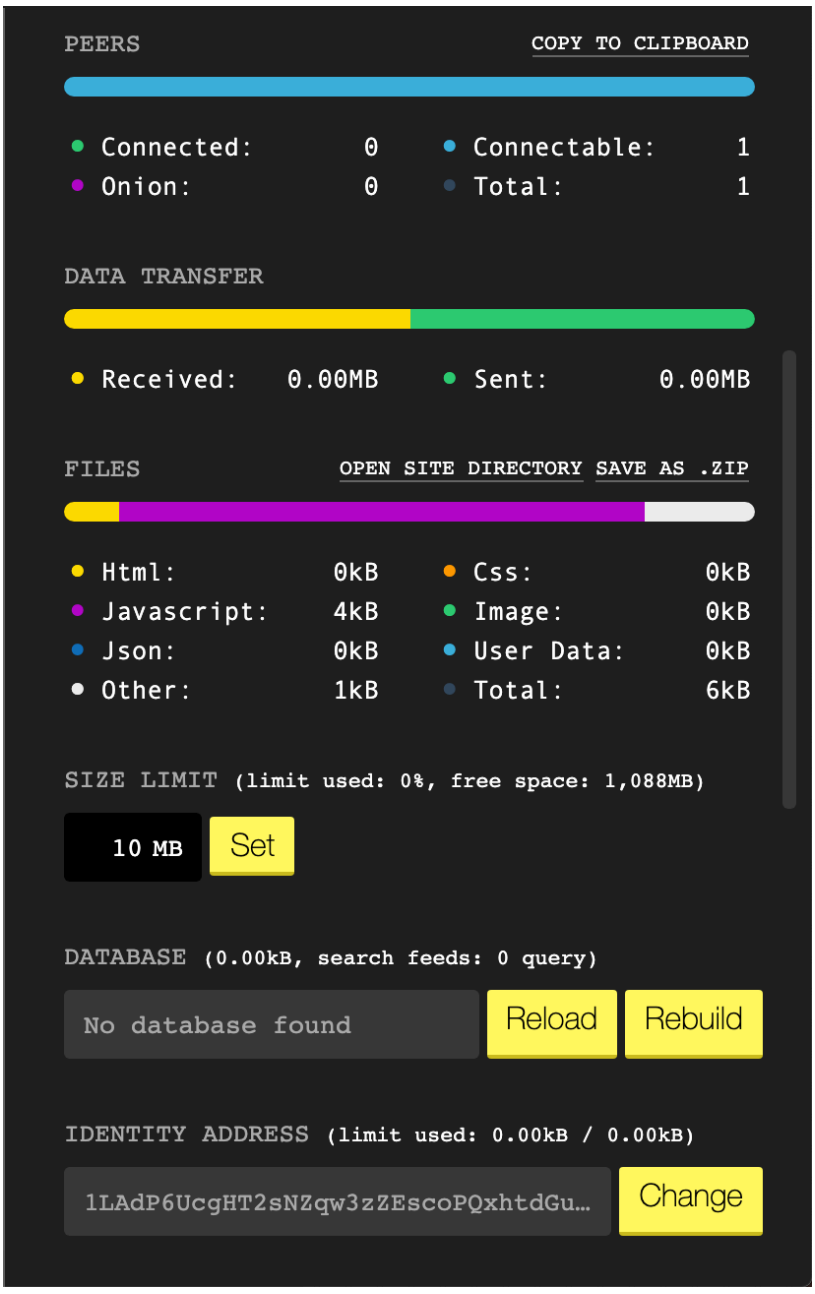

Figure 14 : Tableau de bord d'un site ZeroNet

Dans ce tableau de bord, des statistiques renseignent l'utilisateur sur l'utilisation de son site. Il est également possible de modifier plusieurs paramètres :

- La taille maximale que le site a le droit d'utiliser
- La base de données liée au site
- L'adresse du site
- Le nom du site
- La description du site

Il est également possible, via ce tableau de bord, de mettre à jour le site, de le mettre en pause ou encore de le supprimer définitivement.

Il est intéressant de noter qu'en quelques minutes, moyennant quelques connaissances basiques d'informatique, tout le monde peut participer à un web décentralisé en ajoutant sa pierre à l'édifice en la forme d'un site web.

Dans cet exemple, le site ne sera qu'un site d'information qui contient des données statiques mais en passant plus de temps sur le développement et en s'appropriant les API misent à disposition par ZeroNet, il est possible de créer des sites dynamiques qui n'ont rien à envier aux sites classiques disponibles sur le web actuel.

5. Conclusion

Durant cette recherche, nous avons pu nous apercevoir à travers plusieurs statistiques que les GAFA ont réellement une mainmise totale sur le web actuel. En effet, que cela soit le nombre ahurissant d'utilisateurs sur Facebook ou encore le monopole quasi-total de Google dans le domaine de la recherche, ces entreprises ne laissent que des miettes aux compétiteurs.

Dans l'absolu, cela ne représente pas tant que ça un problème car les services mis à disposition par ces entreprises sont excellents. Le problème est malheureusement ailleurs.

La puissance accumulée par ces entreprises ont fait ressortir leurs mauvais côtés et cela pose de gros problèmes. Google tue toute innovation en rachetant immédiatement n'importe quelle entreprise qui voudrait leur faire de l'ombre. Pour Amazon et Apple, les conditions de travail de leurs milliers d'employés sont le principal problème. Enfin, pour Facebook, l'utilisation de nos données personnelles laisse à désirer et font donc grandir un sentiment de méfiance envers ces entreprises.

Ces points ne représentent qu'une petite partie du problème que représente le web centralisé actuel. En effet, la structure de ce dernier permet également une censure et une surveillance des gouvernements sur leurs citoyens. Un espace qui devait donc être libre et décentralisé se retrouve être un espace surveillé et très centralisé.

Heureusement, plusieurs personnes travaillent sur des solutions afin de proposer un web libre. Cette liberté doit passer par une décentralisation totale des activités du web.

C'est la proposition des projets Freenet et ZeroNet qui utilisent un protocole déjà bien connu, le P2P, afin de décentraliser les sites et de rendre les utilisateurs à la fois clients et serveurs. De cette manière, la liberté est totale, la censure et la surveillance sont rendus quasiment impossible et les services n'appartiennent à personne.

Il existe également d'autres projets, notamment Tor, qui œuvrent pour que tout un chacun puisse naviguer le web de manière totalement anonyme. Certains gouvernements souhaitent également réduire la puissance de ces mastodontes en créant des lois ou encore en définissant une stratégie numérique axée sur plusieurs années.

Le sentiment est le même partout et est partagé par plusieurs personnalités influentes, notamment Tim Berners-Lee, l'un des créateurs du web : Il faut redécentraliser le web ![40]

Les enjeux sont nombreux, autant économiques qu'environnementaux ou encore sociaux mais il est important que le web du futur ne continue pas dans la route empruntée actuellement.

Les projets abordés dans ce travail ne seront peut-être pas la solution adéquate afin de résoudre ces problèmes mais ils représentent une première approche intéressante.

A l'image des crypto-monnaies qui viennent bousculer l'économie avec une technologie complètement décentralisée, peut-être que la technologie des chaines de blocs représente également le futur du web dans quelques années.

Peu importe quelle technologie sera choisie afin de faire avancer le web dans la bonne direction, il est important pour l'humanité d'avoir accès à une plateforme démocratique, sans censure et sans surveillance.

Je terminerai ce travail par citer Tamas Kocsis, le fondateur de ZeroNet[41] :

> *J'ai peur que le futur du web soit hors de notre contrôle. La centralisation croissante et les propositions de lois menacent notre liberté d'expression et, par la même occasion, notre démocratie.*
>
> *Pour moi, créer un réseau décentralisé, c'est créer un refuge, où les règles ne sont pas écrites par des multinationales ou des partis politiques, mais par le peuple.*

[40] https://techcrunch.com/2018/10/09/tim-berners-lee-is-on-a-mission-to-decentralize-the-web/

[41] https://www.ted.com/talks/tamas_kocsis_the_case_for_a_decentralized_internet

6. Bibliographie

Staltz, André Staltz, 30 octobre 2017, The web began dying in 2014, here's how. [Consulté le 2 août 2021] Disponible à l'adresse suivante : https://staltz.com/the-web-began-dying-in-2014-heres-how.html

The Guardian, 12 mars 2017, Tim Berners-Lee: I invented the web. Here are three things we need to change to save it. [Consulté le 2 août 2021] Disponible à l'adresse suivante : https://www.theguardian.com/technology/2017/mar/11/tim-berners-lee-web-inventor-save-internet

Staltz, André Staltz, 18 décembre 2017, A plan to rescue the web from the internet. [Consulté le 3 août 2021] Disponible à l'adresse suivante : https://staltz.com/a-plan-to-rescue-the-web-from-the-internet.html

YouTube, Tedx Talks, 15 juin 2018, It's time to build our own internet | André Staltz | TEDxGeneva. [Consulté le 3 août 2021] Disponible à l'adresse suivante : https://www.youtube.com/watch?v=UjfWAbGfPh0&t=1s

Techjury, Christo Petrov, 14 mai 2021, 52 gmail statistics to show how big it is In 2021. [Consulté le 3 août 2021] Disponible à l'adresse suivante : https://techjury.net/blog/gmail-statistics/#gref

Internet Live Stats, Total number of websites. [Consulté le 3 août 2021] Disponible à l'adresse suivante : https://www.internetlivestats.com/total-number-of-websites/

Hubspot, Victoire Gué, 29 décembre 2020, Les chiffres YouTube à connaître en 2021. [Consulté le 4 août 2021] Disponible à l'adresse suivante : https://blog.hubspot.fr/marketing/chiffres-youtube

Datanyze, Market Share in File Sharing. [Consulté le 5 août 2021] Disponible à l'adresse suivante : https://www.datanyze.com/market-share/file-sharing--198/google-drive-market-share

Datanyze, Market Share in Mapping. [Consulté le 5 août 2021] Disponible à l'adresse suivante : https://www.datanyze.com/market-share/mapping-and-gis--121/google-maps-api-market-share

Statcounter, août 2021, Browser market share worldwide. [Consulté le 7 août 2021] Disponible à l'adresse suivante : https://gs.statcounter.com/browser-market-share

ISU Corp Software, 3 décembre 2020, The best navigation app: Apple Maps vs. Google Maps. [Consulté le 8 août 2021] Disponible à l'adresse suivante : https://www.isucorp.ca/blog/the-best-navigation-app-apple-maps-vs-google-maps

T4, 23 janvier 2021, Email Client Market Share. [Consulté le 9 août 2021] Disponible à l'adresse suivante : https://www.t4.ai/industry/email-client-market-share

Enlyft, Companies using Apple Cloud. [Consulté le 10 août 2021] Disponible à l'adresse suivante : https://enlyft.com/tech/products/apple-icloud

Oberlo, Audrey Liberge, 3 mars 2021, Les 10 chiffres Instagram pour les entrepreneurs. [Consulté le 11 août 2021] Disponible à l'adresse suivante : https://www.oberlo.fr/blog/chiffres-instagram#:~:text=En%202021%2C%20Instagram%20compte%201,%25)%20utilisent%20le%20r%C3%A9seau%20social.

Statista, Statista Research Department, juillet 2021, Most popular global mobile messenger apps as of July 2021, based on number of monthly active users. [Consulté le 12 août 2021] Disponible à l'adresse suivante : https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/

RepricerExpress, Chris Dunne, 15 Amazon statistics you need to know in 2021. [Consulté le 13 août 2021] Disponible à l'adresse suivante : https://www.repricerexpress.com/amazon-statistics/

Statista, Julia Stoll, avril 2021, Number of Netflix paid subscribers worldwide from 1st quarter 2013 to 1st quarter 2021. [Consulté le 14 août 2021] Disponible à l'adresse suivante : https://www.statista.com/statistics/250934/quarterly-number-of-netflix-streaming-subscribers-worldwide/

Statcounter, août 2021, Desktop operating system market share worldwide. [Consulté le 17 août 2021] Disponible à l'adresse suivante : https://gs.statcounter.com/os-market-share/desktop/worldwide

Canalys, 29 avril 2020, Global cloud services market Q1 2021. [Consulté le 18 août 2021] Disponible à l'adresse suivante : https://www.canalys.com/newsroom/global-cloud-market-Q121

PentaBlog, Frédéric Lasnier, 11 décembre 2019, Too big to succeed? How do you solve a problem like GAFA. [Consulté le 19 août 2021] Disponible à l'adresse suivante : https://www.pentalog.com/blog/strategy/gafa-dominates-digital-landscape

The Guardian, Michael Sainato, 5 février 2020, "I'm not a robot" : Amazon workers condemn unsafe, grueling conditions at warehouse. [Consulté le 20 août 2021] Disponible à l'adresse suivante : https://www.theguardian.com/technology/2020/feb/05/amazon-workers-protest-unsafe-grueling-conditions-warehouse

Wikipedia, 30 juillet 2021, Scandale Facebook-Cambridge Analytica. [Consulté le 21 août 2021] Disponible à l'adresse suivante : https://fr.wikipedia.org/wiki/Scandale_Facebook-Cambridge_Analytica

The Guardian, Brian Merchant, 18 juin 2017, Life and death in Apple's forbidden city. [Consulté le 22 août 2021] Disponible à l'adresse suivante : https://www.theguardian.com/technology/2017/jun/18/foxconn-life-death-forbidden-city-longhua-suicide-apple-iphone-brian-merchant-one-device-extract

Influenceurs du web, Carine Panassié, Internet, un espace de liberté ou la censure est reine ? [Consulté le 23 août 2021] Disponible à l'adresse suivante : https://influenceursduweb.org/internet-un-espace-de-liberte-ou-la-censure-est-reine/

Ritimo, Equal Times, 22 mai 2020, Couper et censurer internet : un outil de répression de plus en plus complexe et répandu. [Consulté le 24 août 2021] Disponible à l'adresse suivante : https://www.ritimo.org/Couper-et-censurer-internet-un-outil-de-repression-de-plus-en-plus-complexe-et

Wikipedia, 17 août 2021, Censure d'Internet. [Consulté le 25 août 2021] Disponible à l'adresse suivante : https://fr.wikipedia.org/wiki/Censure_d%27Internet

OpenNet Initiative, septembre 2013, Résultats des recherches. [Consulté le 26 août 2021] Disponible à l'adresse suivante : https://opennet.net/research/data

FramaCloud, L'auto-hébergement. [Consulté le 27 août 2021] Disponible à l'adresse suivante : https://framacloud.org/fr/auto-hebergement/intro.html

Ted, Tamas Kocsis, septembre 2018, The case for a decentralized internet. [Consulté le 28 août 2021] Disponible à l'adresse suivante : https://www.ted.com/talks/tamas_kocsis_the_case_for_a_decentralized_internet

ZeroNet [Consulté le 31 août 2021] Disponible à l'adresse suivante : https://zeronet.io/

Namecoin [Consulté le 31 août 2021] Disponible à l'adresse suivante : https://www.namecoin.org/

Numerama, Alexis Piraina, 13 mars 2016, ZeroNet ouvre la voie à un web vraiment décentralisé. [Consulté le 1er septembre 2021] Disponible à l'adresse suivante : https://www.numerama.com/tech/151860-zeronet-ouvre-la-voie-a-un-web-decentralise.html

TIME, Nikitha Sattiraju (Bloomberg), 2 avril 2020, The secret cost of Google's Data Centers : Billions of gallons of water to cool servers. [Consulté le 2 septembre 2021] Disponible à l'adresse suivante : https://time.com/5814276/google-centres de données-water/

Nature, Nicola Jones, 12 septembre 2018, How to stop data centers from gobbling up the world's electricity. [Consulté le 3 septembre 2021] Disponible à l'adresse suivante : https://www.nature.com/articles/d41586-018-06610-y

Liberation, Christophe Alix, 18 juillet 2018, Android : Google condamné par Bruxelles à 4,3 milliards d'euros d'amende. [Consulté le 5 septembre 2021] Disponible à l'adresse suivante : https://www.liberation.fr/planete/2018/07/18/android-google-condamne-par-bruxelles-a-43-milliards-d-euros-d-amende_1667423/

DigitalDialog, Stratégie Numérique Suisse. [Consulté le 6 septembre 2021] Disponible à l'adresse suivante : https://www.digitaldialog.swiss/fr/

freeCodeCamp, Nader Dabit, 19 mai 2021, What is Web3 ? The decentralized internet of the future explained. [Consulté le 10 septembre 2021] Disponible à l'adresse suivante : https://www.freecodecamp.org/news/what-is-web3/

YouTube, Les Echos, 7 avril 2018, Voici pourquoi vos données personnelles intéressent tant les GAFA. [Consulté le 21 août 2021] Disponible à l'adresse suivante : https://www.youtube.com/watch?v=2h86lnDv2PQ

ZeroNet, Create new ZeroNet site. [Consulté le 11 septembre 2021] Disponible à l'adresse suivante : https://zeronet.io/docs/using_zeronet/create_new_site/

Wikipedia, Internet [Consulté le 11 août 2021] Disponible à l'adresse suivante : https://fr.wikipedia.org/wiki/Internet