Les dangers du numérique

Boris Haguenin, Killian Gajac, Yanis Lacluche

lien de l'image : https://www.flickr.com/photos/143601516@N03/29723649810

Introduction

À la toute fin des années 80, le World Wide Web (WWW) voit le jour. Cette nouvelle innovation majeure est l'une des raisons qui expliquent la popularisation et la diffusion d'internet au milieu des années 90 auprès du grand public. Durant cette période, le Web se voit organisé autour de forums: des sites ayant un/des sujet(s) permettant l'interaction entre les différentes personnes par le biais de chats ou de posts. Avant les années 2000, la publicité sur les sites existe, mais n'est pas une source de revenus très élevée, ni particulièrement favorable, les diffuseurs de publicité n'appliquant pas de réelle restriction sur les publicités qu'ils peuvent proposer.

À l'arrivée de Google AdSense en 2003 (Google AdSense est un service proposé par Google qui permet de facilement intégrer de la publicité à ses sites. Le service permet à Google d'élargir son nombre d'utilisateur pour pouvoir mieux vendre le service à d'autre grandes entreprises, et pour les utilisateurs, ils reçoivent une compensation en fonction du trafic sur leur site.), puis l'arrivée de géants du web comme Facebook, Instagram (Meta), X (anciennement Twitter), Amazon, Youtube et encore plein d'autres, le Web subit alors une première transformation majeure, une centralisation du trafic vers des méga-sites. Cette centralisation apporte avec elle une nouvelle manière de financer l'infrastructure physique et les développeurs de ces sites. Avant AdSense, les différents diffuseurs de publicité sur le Web vendaient simplement leur nombre de sites les utilisant, sans pouvoir donner de garanties sur la portée qu'auront les pubs. Ici Google propose une autre approche pour mettre en valeur leur tout nouveau service. AdSense ne propose pas seulement aux annonceurs, un nombre, mais un outil leur permettant de choisir la cible de leur publicité. AdSense permet alors d'offrir aux annonceurs une sorte de garantie sur le public visé.

Cette évolution, et la rapide prise de pouvoir des publicités sur le Web ont vite éclipsé les autres moyens de financement. Mais pour pouvoir garantir un public cible, Google a dû aussi faire évoluer son objectif. Comme pour les autres géants du Web, Google ne propose plus seulement un indexeur de pages web (Google Search), une plateforme de diffusion de vidéos (YouTube), ou encore des systèmes d'exploitation (Chrome OS, Android). À l'aide de ces outils, Google récupère aussi des informations personnelles sur ses utilisateurs. Cela passe par les différentes recherches de l'utilisateur, au contenu qu'il regarde, en somme les habitudes de consommation de l'utilisateur.

Dans ce document, nous allons découvrir comment les données personnelles sont devenues, en 20 ans, une nouvelle source de revenus majeure. Pour cela nous montrerons les différents outils utilisés par les entreprises du Web, pour récolter de la donnée personnelle, l'utilité pratique de nos données pour les entreprises et les différents moyens que nous avons à notre disposition pour limiter cette récolte à notre égard. Dans un second temps, nous montrerons les dangers d'une telle récolte. Pour cela nous analyserons les failles du système actuel, comment il peut être utilisé pour manipuler. Mais aussi comment les géants du secteur mettent en danger leurs utilisateurs, et aussi les fondations même du Web. Dans une dernière partie, nous discuterons des futurs dangers et évolutions auxquels le Web aura à faire face dans quelques années.

I -La course aux données ou comment alimenter une industrie intrusive à la limite de l'éthique

I.1 - Nos données, sont-elles et comment sont-elles récoltées ?

I.1.1 - Les différentes type de données récoltés

Aujourd'hui, internet n'est plus le havre de liberté et d'expression qu'il était dans ses jeunes années. Le capitalisme et les règles de notre société ont su s'infiltrer dans le monde numérique pour imposer ses lois et ses manières. C'est ainsi que des acteurs du milieu, toujours plus avides de votre attention, se sont attaqués à une nouvelle ressource convoitée, vos données. Elles représentent le nerf de la guerre pour beaucoup de grandes entreprises, elles sont ce qui permet de tout savoir des futurs ou actuels clients. Ces données sont de sources et de types variés selon le secteur concerné. Il y a cependant des données plus communément recherchées que les autres du fait qu'elles donnent des renseignements précieux malgré le fait qu'elles puissent nous paraître bénignes à révéler (voir biblio 7). L'âge fait partie d'une de ces données très convoitées. Cette simple information peut inférer sur vos goûts, vos orientations politiques, vos habitudes d'achats, vos budgets mais aussi les comportements vis-à-vis du numérique et tout cela simplement avec votre âge qui est souvent public et trouvable en ligne pour un grand nombre d'entre nous. Le nom permet de faire des relations entre différentes personnes et de croiser les différentes informations pour en savoir plus sur la personne. On obtient aussi le sexe de la personne, souvent l'origine géographique, les comptes de réseaux sociaux et l'historique professionnel. L'adresse permet d'avoir une idée de votre niveau de vie, de votre environnement social et peut donner une idée de vos habitudes de consommation. Le numéro de téléphone permet d'indiquer votre pays et région, votre opérateur et est une voie facile pour envoyer des infos avec du spam ou faire du reciblage. Du même genre, les mails sont convoités pour les spams. Ce sont les données qu'on désigne comme basiques qui peuvent être exploitées par plus ou moins toutes les entreprises, mais il existe des données plus spécifiques recherchées par des entreprises plus spécialisées et qui valent aussi leur pesant d'or aux yeux des promoteurs. Certaines données valent plus que d'autres car elles sont des indicateurs précis des intérêts que pourrait avoir l'utilisateur. Ce sont des données comme les recherches en ligne pour lesquelles des entreprises peuvent payer très cher du fait des renseignements précis qu'elles peuvent leur fournir. Dans le même genre de données peuvent se trouver les achats en ligne, le temps passé sur un contenu spécifique et des données récoltées suite à l'utilisation de logiciels particuliers. Là où les données précédentes donnent une idée de profilage ou permettent de faire des liens, celles-ci permettent de vraiment trouver le profil type que l'on souhaite cibler avec son produit. Les données, contrairement à ce qu'on pense généralement, ne se limitent pas à notre intérêt d'achat, elles sont beaucoup plus vastes avec des données beaucoup plus sensibles. Il existe des courtiers en santé qui essaient de traquer plus spécifiquement nos consommations de médicaments ou nos recherches sur les maladies pour les vendre à des compagnies pharmaceutiques pour donner des profils qui pourraient être enclins à acheter un médicament particulier. Dans les données sensibles se trouvent aussi des informations financières, des scores de crédit (solvabilité) et des modes de paiement. Ce sont des données qui sont très populaires auprès des spécialistes du domaine qui les vendent pour

des offres commerciales, des banques et des assurances. Certains divisent nos données personnelles en 4 catégories différentes (voir biblio 35). Les données d'identité qu'on a déjà abordées, qui correspondent au nom, âge, sexe, portable, etc. Ensuite les données d'engagement qui correspondent à nos contenus aimés, nos abonnements et la fréquence de connexions à différents réseaux. Ces informations donnent la possibilité de mesurer l'influence et l'attention de certains contenus sur la personne et des contenus qui devraient l'intéresser. Les données comportementales telles que les historiques de recherche, les achats et les horaires d'activités permettent de faire des modèles prédictifs et de réellement trier les individus par modèle. On essaie de déterminer au mieux les habitudes des utilisateurs. Enfin les données d'attitude qui concernent nos opinions, nos valeurs sociales, politiques ou religieuses et tout ce qui va concerner notre personnalité et notre sensibilité émotionnelle qui vont permettre d'exploiter nos vulnérabilités psychologiques ou influencer nos opinions, elles permettent de persuader à croire en leurs avis. Ces 4 types de données permettent quasiment de tout connaître d'une personne en s'infiltrant dans sa vie privée et son anonymat pour avoir toujours plus son attention,pouvoir ou argent. Maintenant se pose la question de comment ces grands acteurs du marché de la donnée récupèrent des informations sur internet ? Une des méthodes les plus simples et connues, ce sont les cookies.

I.1.2 - Que sont les cookies et comment marchent ils

Les cookies, aussi appelés témoins de connexion en français (voir biblio 34), sont partout sur internet. N'importe quel site, quel qu'il soit, offre un système de cookies à ses utilisateurs et, bien qu'en certains aspects cela soit bénéfique à notre navigation sur internet, son coût est devenu bien supérieur à ses avantages. Dans les faits, les cookies sont de petits fichiers directement stockés sur votre navigateur et donc, par extension, votre propre ordinateur, qui vont fournir des données que le site va pouvoir consulter quand vous le visiterez. C'est une technologie ancienne créée en 1994 et très populaire, désormais utilisée par la moitié des sites sur internet (voir biblio 34). Bien que les cookies aient leur lot d'avantages comme la mémorisation de nos codes d'authentification, la prise du bon langage, et des normes de sécurité, ils ont aussi une part plus sombre avec des cookies commerciaux qui ont pour unique but de recueillir des données sur notre navigation sur le site, notre temps de passage, la quantité d'achats, les articles regardés, etc. Ces cookies permettent de récolter des données sur les utilisateurs et peuvent être ensuite utilisés ou revendus sans que l'utilisateur ne s'en rende forcément compte. Maintenant abordons ce que sont les cookies. On peut les diviser en deux catégories : les cookies internes (aussi appelés « first-party ») et les cookies tiers (aussi appelés « third-party ») (voir biblio 36). Contrairement à ce que beaucoup pourraient croire, les cookies internes et tiers ne signifient pas simplement le fait d'être essentiels ou dispensables, la nuance entre les deux correspond à "où le cookie est déposé". En effet, dans le cas des cookies internes, ils se trouvent directement sur le site consulté et peuvent donc contenir les cookies essentiels ou des cookies à but publicitaire. Les cookies tiers, eux, sont déposés sur un autre domaine que celui du site, ils peuvent aussi être subdivisés en deux genres : les nécessaires pour le fonctionnement du site, mais peuvent aussi servir à collecter des données pour faire de l'annonce plus ou moins de la même manière que les internes. Cependant, généralement les cookies tiers servent surtout à collecter des données à des fins publicitaires et il est plutôt rare qu'un cookie tiers soit nécessaire. Il est aussi important de noter que les deux types de cookies peuvent être soumis à la CNIL, donc l'acceptation ou non d'un cookie n'est pas liée à son origine mais à

son utilité. Rentrons maintenant plus précisément dans le sujet controversé de ces cookies espions communément appelés traceurs. À partir de notre adresse IP qui va servir à nous authentifier, le cookie commercial sur un site unique va récolter des données statistiques comme cité précédemment, mais cela peut aller plus loin. Les cookies tiers peuvent permettre de suivre un utilisateur sur plusieurs sites à la fois, tout simplement en étant mis en tiers sur tous ces sites suivants et ainsi de faire un véritable historique des activités et faire un véritable profilage de l'internaute (voir biblio 8). Les pages web sont constituées de différents objets qui n'existent pas sur le même serveur, comme les images par exemple. Donc, dans ce cas-là, votre navigateur va demander à cet autre serveur de lui fournir ce contenu qui peut venir aussi avec son lot de cookies. Dans les faits, c'est à ceci que correspondent les cookies tiers. Étant très contestés et portant souvent atteinte à la vie privée, certains navigateurs permettent de s'en protéger et même Google avait essayé de s'en prévenir d'ici 2022 sans que leur projet n'aboutisse. Actuellement l'utilisation de cookies publicitaires est autorisée avec le consentement de l'utilisateur. Le problème est que peu de gens savent réellement ce que ces cookies signifient et acceptent par méconnaissance.Certains site se sont même développés pour montrer toutes les informations que l'on peut obtenir via une simple connexion afin de montrer toute les informations récoltables d'un simple clic, par exemple le site https://webkay.robinlinus.com permet des données sur votre position ip approximative logiciel hardware etc. De plus, certains sites ont développé de nouvelles techniques pour forcer leurs utilisateurs à les accepter. L'une des techniques les plus utilisées est le « cookie wall » ou mur de traceur qui, en cas de refus de ces cookies non essentiels, refuse l'accès au site tant qu'une autre contrepartie (souvent monétaire) n'est pas acceptée. La CNIL autorise cette pratique mais essaie de la limiter et souhaite réduire au maximum l'utilisation de ce nouveau système qui pousse toujours plus loin le vice des grandes plateformes de sites en ligne (voir biblio 16). Bien qu'il soit possible de s'attaquer à un site qui pratique ce système, il faut passer par le système juridique qui est souvent long et complexe et il devient en pratique de plus en plus dur d'échapper à la surveillance effectuée sur tous nos sites du quotidien avec des techniques toujours plus fourbes comme le pixel espion qui insère un pixel invisible dans votre page pour faire office de cookies sans être remarqué et fonctionne comme les cookies tiers afin de récupérer toujours plus de nos données (voir biblio 34). Nous avons abordé le sujet des cookies, mais ils ne sont évidemment pas les seuls moyens qu'ont les entreprises pour nous surveiller. D'autres méthodes existent pour récolter nos données et nous allons en découvrir quelques-unes.

I.1.3 - Les différents moyens et traceurs pour prendre vos données

Il existe d'autres sources d'information qu'utilisent les entreprises pour s'accaparer vos informations. Ces méthodes sont souvent hétérogènes et multiples. Nous allons voir quelques exemples de ces méthodes. Contrairement à ce qu'on pourrait attendre, les sources gouvernementales sont très utilisées. Loin de nous protéger, le gouvernement fournit en accès libre et gratuit aux brokers une énorme quantité de données (voir biblio 8). Les gouvernements laissent au public l'accès aux actes de naissance et de décès de tous les Français qu'ils recensent . Dans le même genre, nous avons aussi le droit de consulter les actes de mariage et les journaux officiels. Mais ce n'est pas tout, malheureusement il est fréquent que des banques de données de notre gouvernement fuitent et offrent des données. Que ce soit France Travail ou l'Urssaf, les fuites de données sociales ne manquent pas. Les entreprises, elles aussi, fournissent des données en quantité, que ce soit

avec internet ou physiquement. Elles peuvent donner des informations d'achat et sur leurs utilisateurs et même les informations que peuvent fournir les cartes de fidélité. En dehors des cookies, des traceurs existent avec par exemple les inscriptions en ligne qui vont fournir votre adresse e-mail au site, qui se permet souvent de la repartager. Les liens mail permettent aussi de vérifier si un e-mail est en vie et encore utilisé. Il existe aussi les sondages qui sont une source d'informations plus globales sur une population et qui peuvent orienter la création des profils. Mais le système le plus utilisé qui n'est pas des cookies vient des SDK (Software Development Kit, soit Kit de développement logiciel) embarqués dans les différentes applications qu'on utilise. Les SDK sont des outils de développement qui peuvent ensuite s'intégrer dans un logiciel. Ici nous nous intéressons en particulier à ceux qui permettent de récupérer nos données et ensuite de les envoyer à des serveurs liés. Ces SDK sont souvent développés par des grandes entreprises de la tech comme Google, Meta, Amazon, Microsoft et d'autres acteurs du milieu. Une majorité des applications qu'on télécharge sur notre téléphone et certains logiciels PC comportent un programme espion qui récolte des informations, que ce soit notre application météo, GPS ou jeux vidéo, ils permettent de récupérer des données qui sont souvent inutiles au fonctionnement de l'application. De plus, contrairement aux cookies qui demandent notre accord pour accéder à nos informations, les SDK ne demandent aucune action explicite de l'utilisateur, prenant les informations sans aucun accord. Ces informations peuvent concerner des données déjà présentées précédemment comme l'adresse e-mail, le modèle de l'appareil, son OS ou même des informations moins attendues comme la résolution de l'écran, les capteurs. Ces SDK peuvent être louables avec de la détection de bug ou une connexion rapide à votre compte, mais sont souvent le plan financier de ces applications avec la vente des mesures de performance ou la monétisation. Ces applications peuvent aussi accéder, cette fois avec accord de l'utilisateur, à sa caméra, son micro, son stockage et contacts, ce qui, cette fois, en plus de faucher nos données, met à risque nos appareils et peut permettre de connaître des failles dans notre système. Ces SDK sont totalement légaux et en règle avec le RGPD (dont nous parlerons plus tard) mais en pratique leur usage est souvent non conforme ou flou en ce qu'il est difficile de vérifier automatiquement les actions d'une application ou logiciel à grande échelle, ce qui fait que de nombreux développeurs en profitent pour prendre des données sans se faire remarquer. Les réseaux sociaux en particulier ont un suivi de vos informations très poussé car nous livrons directement nos conversations et nos goûts à l'application. L'algorithme pousse des contenus que nous sommes susceptibles d'apprécier grâce à nos propres recommandations que l'on fournit par nos likes qui sont originellement destinés à communiquer à nos amis notre intérêt pour un contenu. Le « watchtime » est aussi une métrique qui va être exploitée et qui, elle, est plus insidieuse mais qui sert à ces réseaux à déterminer nos passions ou intérêts. En acceptant l'usage de ces applications pour communiquer, vous leur fournissez toutes les informations dont ils pourraient rêver sur vous. C'est en fait le principe même de leur application : ce sont ces données qui font leur marché, ce qu'on appelle l'économie de l'attention, ou des pubs qui vous intéressent seront ensuite partagées via leur réseau grâce aux infos fournies par vos propres messages ou communiqués (voir biblio 9). Maintenant qui s'occupe de traiter, acheter ou revendre ces données pour gérer ce marché juteux qui, on estime, pèserait autour des 184 milliards d'euros ? Ce sont les data brokers, les titans silencieux du monde de l'entreprise qui font vivre ce marché de l'intrusion.

Dans la prochaine partie, nous explorerons cette partie cachée de notre économie.

I.2 - Data broker et marché de l’attention quand vos données deviennent monnaies

I.2.1 - Qui sont les data broker ?

Abordons le sujet des data brokers, que l’on nomme en français les courtiers en données/informations (voir biblio 8). Ces entreprises dont le nom nous est inconnu mais qui valent des milliards, avec par exemple Acxiom, une des plus grandes sociétés de la data avec un chiffre d’affaires de 1.15 milliards de dollars par an dès 2012 (voir biblio 38) et une base de données de 2,5 milliards de consommateurs (voir biblio 37). Maintenant déterminons ce que sont les data brokers, métier apparu dans les années 50. Le métier commence à faire vraiment parler dans les années 90 (voir biblio 8). Ce sont des personnes ou entreprises qui ont pour objectif de collecter et trier des données afin de les revendre généralement à des annonceurs, même si les clients peuvent être divers. Internet a bouleversé ce milieu qui autrefois se servait énormément des documents publics pour trouver ces informations. Ils ont commencé à utiliser de plus en plus de données privées et récupérées depuis différentes plateformes et ont grandi pour devenir les géants de l’industrie de maintenant. Les sources se sont diversifiées, les données aussi, comme décrit précédemment, et certains se sont même spécialisés dans la vente de certains types de données. Ce marché est très controversé et souffre d’un manque d’éthique et de transparence sur leurs agissements qui restent souvent impunis au vu des sommes et des entreprises impliquées. C'est un réseau très fermé qui regroupe les plateformes de réseaux sociaux, des banques, des médias, des assurances, mais aussi des acteurs politiques. Ils vont d’abord récolter les données avec les différentes manières déjà explicitées puis vont les classer dans des dossiers. Avec ce qu’ils ont récolté, leur objectif va être de recouper les informations disponibles et d'utiliser les différentes données à leur disposition pour faire le profil d’une personne en le recomposant pour le mettre dans un dossier (une base de données) de personnes qui lui correspondent. Ce dossier sera vendu à l’acheteur selon ses besoins avec les profils associés à sa demande. On transforme les vies privées des individus en chiffres et en classeurs pour le profit. Les clients y gagnent car ils sont plus sûrs de faire des ventes sur ces profils qui sont déjà intéressés par leurs produits et les vendeurs gagnent en échange de grandes sommes d’argent. Ils appellent ces profils des « persona » et se concentrent souvent sur des points commercialement stratégiques. Peu de réglementations encadrent et limitent ces entreprises, surtout aux états-Unis où la protection de la vie privée est quasi nulle. Il est difficile de savoir lesquelles de nos données privées sont devenues publiques et achetables par différents clients. Avec le temps, l’intelligence artificielle a fini par s’implanter dans une part importante de la profession. En effet, les IA génératives du genre LLM et autres ont besoin de données en grande quantité pour leur entraînement, des données souvent extraites du big data, dont fait partie celles que possèdent les courtiers en informations. Il existe aussi des scandales liés à d’autres types d’IA qui ici exploitent les données des courtiers pour influencer des opinions à grande échelle, ce qui a encore poussé la controverse sur l’utilisation frauduleuse qui englobe les données avec des événements et des IA comme Ripon ou Facebook-Cambridge Analytica

dont nous discuterons plus tard dans le document. Ces données peuvent avoir un effet positif comme la détection de fraude, mais leur usage est souvent malveillant et à but lucratif. Le marché de la vente de données est en croissance constante avec des prévisions autour de 600 milliards de données d'ici 2030 (voir biblio 39). Les acteurs se multiplient avec dans le monde autour de 4000 à 5000 data brokers (voir biblio 39) qui se partagent le domaine avec des géants de l'ombre tels que Acxiom, considéré leader du marché, mais aussi Experian, Equifax ou Epsilon qui dominent le milieu. Maintenant parlons plus précisément des acheteurs du marché et du ressentiment de fraude qui entoure ce domaine. Comment appliquent-ils la connaissance de nos données pour la transformer en profit ?

I.2.2 - Qui achète ces données et que faire avec ?

Nos données sont précieuses et de nombreuses entités sont prêtes à dépenser énormément d'argent pour les obtenir. Mais comment s'en servent-elles concrètement ? En quoi est-ce préjudiciable pour nous ? Qui les achète ? Répondons à ces questions. Les clients avides de données sont souvent des grandes industries et pas toujours les plus attendues, par exemple des agences gouvernementales qui les utilisent pour obtenir des données sans recourir à des procédures judiciaires interminables ou pour la surveillance et la sécurité nationale avec des exemples comme la police ou de la géolocalisation ou des informations de réseaux sociaux, l'immigration pour la vérification d'identité, la fiscalité pour la détection de fraudes. Il y a aussi des scientifiques en sciences sociales qui en ont besoin pour confirmer leurs théories, tester des théories à grande échelle, ou avoir accès à des populations difficiles à observer et étudier des comportements réels sans biais. Des partis politiques pour du micro ciblage électoral, essayer de trouver des indécis et adapter son discours par rapport au profil qui leur correspond. Ou enfin des organisations à but non lucratif qui veulent maximiser leur impact ou trouver des personnes à recruter. Il y a aussi des profils plus communs comme les banques pour compléter des dossiers de nouveaux potentiels clients, évaluer le risque de crédit sur certains individus. Les assureurs pour sensiblement les mêmes raisons. Les réseaux sociaux qui d'ailleurs achètent et produisent des données les achètent pour enrichir leur profil et améliorer leur ciblage publicitaire. Les médias, pour optimiser pub et audience, recherchent toujours plus de contenus personnalisés et se concentrent sur les sujets qui intéressent le plus grand nombre de personnes. Les industries de la recherche d'emploi pour vérifier ses candidats ou le calcul de performance. Il y a aussi d'autres grandes entreprises privées qui peuvent devenir clientes pour diverses raisons. Ces clients sont triés sur le volet pour éviter que des fuites de données ne puissent arriver, même si des criminels ont déjà réussi à le faire en se faisant passer pour différentes instances, ce qui a conduit à de grands vols d'identité ou à des fuites de données qui mettent à risque un grand nombre de personnes avec des données toujours plus nombreuses et privées comme des données bancaires qui peuvent finir sur des sites illégaux et être récoltées par le premier venu ou revendues à des organismes criminels (voir biblio 8). L'utilisation de ces données nous met dans un monde de probabilités où l'individu n'est plus considéré dans la masse. S'y ajoutent une traçabilité de notre personne toujours plus grande, qu'elle soit physique ou numérique, et une véritable disparition de notre anonymisation sur internet où tout est espionné et nos actions deviennent traçables de site en site jusqu'à notre vraie identité. Et tout ça sans que l'on puisse savoir concrètement ce que l'on sait de nous sans passer par des demandes compliquées et qui peuvent elles aussi nous laisser avec une réponse incomplète à cause de la discrétion dont font preuve ces entreprises dans leur vol de données. Nos données peuvent aussi nous enfermer dans une

bulle, prisonniers de nos propres données, une manipulation douce et constante de nos informations et une vraie perte d'autonomie. Ce qui nous amène à notre prochain point, un aperçu de l'économie de l'attention et son utilisation des données, notamment avec des exemples venus des réseaux sociaux et leur manière toxique de faire du business.

I.2.3 - L'attention quand vos données deviennent de l'or

L'économie de l'attention est un marché où votre temps est leur argent. C'est le marché que manipulent les réseaux sociaux et qui exploite les données personnelles pour prendre un maximum de votre attention, votre temps en somme. Les réseaux sociaux ont un système monétaire simple, celui de la publicité. Chaque publicité visionnée via leur plateforme leur rapporte une petite somme d'argent qui, cumulée, forme de véritables monticules, et c'est ce système qui a permis à des groupes comme Facebook de devenir gigantesques aussi rapidement. Maintenant un problème se soulève, les publicités ne correspondent pas forcément à l'utilisateur et il peut lui arriver de quitter le site. Vient alors en jeu le marché de l'attention. Les réseaux sociaux se sont mis à développer des systèmes pour avoir toujours plus de temps d'utilisation, ils se sont mis à exploiter des techniques néfastes proches de celles du casino pour essayer de gagner de plus en plus de parcelles de votre journée. Pour essayer de reproduire l'effet de dopamine que représente une victoire dans un casino, leur algorithme est fait de sorte à proposer des contenus moyennement, voire peu intéressants sur commande pour pouvoir garder le spectateur captivé jusqu'au prochain contenu susceptible de vraiment lui plaire. C'est ainsi qu'on obtient un effet où les gens se mettent à « scroller » pendant des heures pour trouver leur dose de dopamine à laquelle ils sont devenus accros (voir biblio 1). Leur objectif est de créer une véritable dépendance à leur application, ils veulent instaurer une routine qui ensuite se partagera à vos amis par effet de groupe. Pour forcer cette addiction, les réseaux poussent le plus possible les contenus polarisés pour générer le plus de réactions possible et les contenus rapides et consommables qui n'offrent pas de véritable réflexion sont donc mis sur un piédestal. On noie le consommateur sous du contenu et on envoie le plus de notifications pour toujours rappeler ce nouveau besoin d'aller sur ces réseaux. Ce n'est pas la seule chose répréhensible que font les réseaux sociaux. Chaque discussion que vous partagez sur leur application leur est techniquement en accès libre et ce grâce à leur condition d'utilisation qui fait d'eux les maîtres de vos informations, comme nous l'avons expliqué précédemment. Des fois les entreprises des réseaux sociaux brisent même les lois, comme YouTube très récemment, qui passe par-dessus les limites imposées par l'Europe pour déterminer si un adblocker était installé sur votre navigateur pour bloquer le visionnage le cas échéant (voir biblio 40). Ces réseaux se rapprochent petit à petit de la limite et la dépassent même parfois, et les limites de leur modèle commencent à se voir, les gens passent déjà une quantité trop grande de temps sur les réseaux et les acteurs se battent entre eux pour le peu de temps qui reste. Un jour ce modèle économique se verra ralentir et décroître, ce qui poussera peut-être ces entreprises à exploiter nos données d'une manière encore plus révélatrice. Maintenant, que pouvons nous faire pour essayer de nous protéger y a t'il des moyens de se prémunir du vol de données? Trouvons des réponses dans la prochaine partie.

I.3 - Comment protéger nos données et nos droits

I.3.1 - le manque de prévention du grand public

De nos jours beaucoup de nos droits en informatique sont fragiles, ils sont méconnus du grand public qui se soucie rarement de problèmes juridiques et qui requiert souvent une expertise ou connaissance non accessible au citoyen moyen. Le public ignore souvent ce que signifient les cookies et l'implication de l'acceptation de ceux-ci, se laissant donc collecter leurs données. Avec l'apparition en plus de nouvelles méthodes pour forcer les gens à utiliser les cookies, les quelques résistants se résignent et cèdent aux entreprises qui profitent d'une architecture volontairement opaque qui brouille encore le droit à nos contrôles sur nos données. Les services qui exploitent ces techniques sont devenus un nouveau besoin, ils sont devenus indispensables à un grand nombre d'entre nous, ce qui nous oblige à cesser la résistance. Il est quasi impossible de protéger toutes ces données. Le lobbying a fait entrer progressivement le vol de données dans la construction de nos infrastructures logicielles. Aujourd'hui tout le monde est à risque, mais surtout les plus jeunes et les plus âgés. Nos benjamins se sont construits autour d'internet et d'applications et de réseaux sociaux qui volent nos données. Le regard social a poussé une grande partie de cette génération dans les bras des réseaux avec un système déjà bien établi qui ne permet pas de voir les problèmes sous-jacents. Ce système a aussi fait baisser le niveau en informatique. Les simplifications modernes ont fait que les jeunes maîtrisent en fait moins bien les outils informatiques que leurs aînés et ne comprennent pas vraiment les machines qu'ils manipulent pourtant toute la journée. Ce sont aussi des esprits qui manquent encore de recul et qui ne sont pas encore prêts à réellement défendre leur droit, ils sont donc devenus les nouvelles cibles et les produits de demain. Nos doyens, quant à eux, font face à leur manque de connaissances dans l'informatique et sont globalement moins à l'aise avec le numérique. Beaucoup d'entre eux ont une confiance aveugle dans les interfaces qu'on leur met en place et sont trop crédules par rapport aux informations qu'on leur transmet et sont facilement manipulables par les nouvelles technologies. Malgré l'introduction du RGPD ou de moyens de se protéger, peu de personnes sont au courant de leurs droits et nos compatriotes restent bloqués dans le système des courtiers en données et leur espionnage de masse industrialisé. Maintenant que nous sommes avertis du manque de connaissance, comment se prévenir de tout vol de données ?

I.3.2 - Que faire face aux cookies ?

Certaines lois sont là pour nous aider à protéger nos données. La CNIL met à disposition des moyens de défendre sa vie privée et d'autres services permettent aussi d'utiliser internet en gardant son anonymat (voir biblio 19). Tout d'abord le choix de votre navigateur est important, un grand nombre de navigateurs ont pour chiffre d'affaires la vente de données et de pubs ciblées, mais certains prennent une autre alternative. Les navigateurs les plus populaires sont très indiscrets et récoltent énormément de données, par exemple des navigateurs comme Chrome, Microsoft Edge ou Firefox qui récoltent de plus en plus de données. Il vaut mieux choisir pour plus de sécurité de vos données des logiciels comme TOR qui anonymise complètement son utilisateur (à la condition de ne pas lier son compte)

et pour des utilisations plus usuelles des navigateurs comme Brave qui ont une politique claire sur la récolte d'informations personnelles. Les paramètres de nombreux navigateurs populaires permettent tout de même de désactiver les cookies tiers dans des sous-menus, les moyens de les désactiver sur chaque navigateur sont disponibles sur le site de la CNIL (voir biblio 20). Un VPN peut aussi servir à vous aider dans la conservation de vos données, il permet de cacher votre vraie adresse IP qui pourrait être récoltée pour déterminer votre localisation, il chiffre vos données et rend difficile la récolte d'informations. Les bloqueurs de pubs sont aussi une alternative de protection en bloquant les traqueurs publicitaires comme les cookies ou pixels espions, stoppent le « fingerprinting », technique qui permet de déterminer le navigateur et l'appareil utilisés, et enfin empêchent l'apparition de pubs ciblées sur votre page. On peut aussi directement supprimer sur notre machine, effacer les cookies déposés pour retirer les éventuels cookies déjà enregistrés et qui ne sont pas nécessaires. À noter que cela supprimera vos connexions déjà enregistrées sur certains sites et forcera une reconnexion. Certaines procédures peuvent aussi être utilisées pour conserver nos données. La loi est aussi un moyen efficace grâce à plusieurs droits : celui à l'effacement complet, qui est le droit à l'oubli, celui d'opposition, qui permet de refuser l'usage de données à but commercial, le droit d'accès, qui permet de voir les données qu'un site possède sur nous, et enfin le droit de rectification, qui permet de corriger une donnée. Ce sont des droits qui font partie du RGPD, qui est le règlement général sur la protection des données en Europe. Les sites ciblés par des demandes concernant ces droits se doivent d'accéder à la demande. Dans le cas où ils ne procèdent pas sous 30 jours, la CNIL pourra vous aider à porter votre cause. Il existe des outils qui permettent d'automatiser ces demandes RGPD comme Incogni, OneRep ou Mine qui permettent respectivement de supprimer les données de site, les données publiques et les données mail. Ce sont souvent des options payantes mais bien plus efficaces en temps et en pratique. On peut aussi demander à Google et aux autres moteurs de disparaître des recherches. Cependant, il est souvent difficile de supprimer les informations des réseaux sociaux, qui peuvent même créer des profils sans que vous soyez actif sur l'un d'entre eux grâce aux messages vous concernant partagés par vos contacts. En effet le RGPD est encore très limité tout comme la CNIL qui l'applique en France, nos droits sont encore partiels et il est difficile sans outils et même avec de les faire appliquer pour réellement être invisible, tout le monde est à risque et même le plus averti ou sécurisé peut finir sur des listes de vendeurs de données.

I.3.3 - Un système défaillant ou trop limité ?

Nous avons clairement un problème dans notre protection des données, beaucoup de trous permettent à un marché intrusif de subsister et même de croître en devenant des géants invisibles de l'économie. Nos politiques sont inconscients de tous les problèmes sous-jacents que pose le manque de vie privée sur internet et se fichent plus ou moins des implications d'internet dans le monde moderne. Les législations sont en retard, le monde politique est lent dans sa prise de décision dans un monde numérique où l'évolution est rapide et constante. Notre quotidien devient davantage connecté et nos droits ne semblent pas progresser en accord avec celui-ci. Ces questions restent secondaires, voire insignifiantes, dans le débat public et certaines lois poussent même vers de nouveaux risques pour notre anonymat et nos données dans l'univers numérique. Il est existentiel de questionner notre rapport au numérique et les lois qui régissent le virtuel afin qu'il ne devienne pas une nouvelle jungle où les entreprises intouchables se battent pour un web liberticide comme nous y tendons actuellement. Dans la prochaine partie, nous aborderons

ce sujet plus en détail avec des exemples et verrons les véritables enjeux derrière le web et son évolution.

II - La mise en danger de la liberté et l'anonymat sur le web

II.1 - La récolte de données, un danger pour les utilisateurs

Cette partie utilise le livre *Le business de la haine* comme source principale (2)

II.1.1 - Une identité numérique créée par les entreprises, pour les entreprises

Comme évoqué dans l'introduction de ce document, l'évolution du financement des sites qui peuplent le WEB est très rapidement passée du bénévolat (où des passionnés créent des petits sites de tout genre) aux dons des utilisateurs du site pour pouvoir légèrement couvrir le prix grandissant des infrastructures. Système très vite abandonné pour laisser place à la publicité, bien plus rentable et facile à mettre en place grâce à l'arrivée d'AdSense. C'est dans ce contexte que la collecte de données personnelles a commencé à devenir de plus en plus commune. L'évolution de la publicité sur le web suit un schéma similaire à celle des journaux. Pour qu'une entreprise touche le plus efficacement possible sa clientèle, elle réalise des études de marché et marketing, puis choisit de mettre en place des publicités dans les journaux ayant le plus de chances de remporter une vente. Depuis l'arrivée de AdSense, Google a créé un service qui permet de choisir à qui, quand, comment sera présentée sa publicité.

Pour assurer aux utilisateurs du service que les publicités seront bel et bien correctement ciblées, Google a mis en place une récolte de données personnelles. Cette récolte de données permet aux entreprises d'obtenir un profil plus ou moins détaillé de l'utilisateur (dépendant du niveau d'intrusion dans la vie privée de l'utilisateur par ses mêmes entreprises). Ce profil permet de mettre l'utilisateur dans différentes cases. Plus l'entreprise récolte de données, plus le profil sera détaillé, ce qui sert ensuite d'argument de vente pour le système de diffusion de publicité. Ici on ne vend plus simplement la quantité de sites utilisant le système de diffusion de publicité, mais aussi la précision de celui-ci. Les entreprises qui récoltent nos données se nomment des courtiers en données. Leur but est simple : savoir tout sur nous. Soit pour leurs services, soit pour utiliser nos données comme monnaie d'échange avec d'autres entreprises.

Si une seule entreprise récoltait nos données, il suffirait de lui refuser le droit, et alors le problème n'existerait pas. Cependant, aujourd'hui, quasiment toutes les entreprises du web réalisent, à plus ou moins grande échelle, cette récolte de données. Elles partagent souvent entre elles le fruit de leurs efforts (contre de l'argent, bien évidemment). Pour les résidents de l'Union européenne, nos données personnelles sensibles sont protégées sous le RGPD. Cela n'empêche pas les entreprises de collecter nos données non sensibles et d'utiliser d'autres méthodes pour quand même nous mettre dans des cases. Pour la plupart des autres pays du monde, il n'y a quasiment aucune règle protégeant l'individu du vol massif de données qu'il subit. Le catalogage des individus est donc encore plus fort dans ces pays.

Malheureusement, le RGPD ne protège pas les utilisateurs de toute récolte de données. Cette récolte peut être aussi simple que de demander à l'utilisateur son numéro de

téléphone pour obtenir de nouvelles fonctionnalités (authentification à double facteur), les fonctionnalités des sites, comme mettre un "j'aime" à une publication, s'abonner à un fil/forum, suivre une personne, les personnes que l'on a en amis. Toutes ces informations ne sont pas soumises aux restrictions du RGPD, puisqu'elles sont "obligatoires" au fonctionnement des sites, cependant ces informations peuvent être utilisées par les sites comme bon leur semble.

II.1.2 - La publicité extrêmement ciblée

Cette récolte de données constante permet aux entreprises de cibler correctement les publicités aux utilisateurs. Les personnes de 15 à 18 ans ne seront sûrement pas très intéressées par des publicités de produits ménagers. Ce ciblage a débuté assez humblement, l'âge, la langue, une localisation large, pouvaient être sélectionnés. Puis cela a évolué pour se spécifier, viser des catégories plus petites, inclure le moins de gens qui risqueraient de ne pas être intéressés. Puis on a pu viser des catégories très précises de gens, comme par exemple les fans de telle équipe de foot, les gens qui ont aimé des publications liés à la politiques, au jeux vidéo, sport, les gens qui réagissent fortement, les gens qui ne réagissent pas, des discussions autour de sujet précis, etc.

Le service de ces entreprises est puissant pour plusieurs raisons. La première étant le nombre de personnes "inscrites" à leurs services. Personne n'est réellement inscrit au service de diffusion de publicité, l'utilisateur du réseau social subit la publicité. Elle lui apparaît devant lui, durant son utilisation du service proposé par le site. Le nombre de personnes touchées est donc énorme, plus le service de diffusion est utilisé par des sites, plus le service touche de monde. Le deuxième facteur est la précision du service. Une entreprise peut choisir avec énormément de précision quelle publicité doit être vue par quel type d'utilisateur. Cela est gagnant pour l'entreprise qui vend le service de diffusion, car une entreprise aura tout intérêt à utiliser au maximum le service, en créant un maximum de publicités différentes.

II.1.3 - Un système pouvant être exploité

Mais ce système n'est pas sans faille. Une entreprise qui tient à vendre un produit a évidemment pour but de maximiser ses profits. D'où pourquoi le système de publicité fut créé. Le problème de ce système provient du fonctionnement même des sites qui les hébergent. La publicité est ciblée à un niveau jamais vu avant. Comme dit précédemment, cette même publicité est imposée à l'utilisateur. S'il utilise le site, des publicités lui seront montrées. C'est le contrat de base de la plupart des sites modernes. Ces sites sont là pour réaliser un profit, pour maximiser le profit, ces sites ont investi une grande partie de leurs bénéfices dans la création d'outils de récolte de données très puissants. De plus, ces sites veulent aussi être les seuls que l'utilisateur utilise. Il doit prendre l'attention, captiver l'utilisateur pour qu'il ne réalise pas le temps qui passe. Ces sites sont donc conçus pour être addictifs. Le problème vient de ce lien entre le fonctionnement addictif du site et le contrat de financement imposé.

La publicité n'est jamais agréable quand elle interrompt une chose que l'on apprécie. Elle frustre, et si elle frustre alors elle n'est pas efficace. Le site est donc construit autour de la publicité, la publicité forge comment le site fonctionne pour que son apparition ne frustre pas l'utilisateur. La publicité doit sembler intégrée, comme élément normal du site. En défilant

des vidéos/images/posts dans notre fil d'actualité, une publicité peut s'y glisser, comme contenu généré par l'utilisateur. Si celle-ci est correctement ciblée, alors elle a de très fortes chances de d'induire à une vente. Il est légalement interdit de dissimuler une publicité, c'est pour cela qu'elles ne le sont pas. Il y aura toujours écrit que le post/vidéo/image est une publicité. Alors comment les sites arrivent à parfaitement l'intégrer ? En étant extrêmement addictif. Quand l'utilisateur est absorbé par le site, il ne réalise plus ce qu'il fait, il réalise des actions par automatisme. Les sites cherchent à pousser tous leurs utilisateurs dans cette phase d'addiction.

Les services proposés par les géants du Web possèdent malheureusement un défaut pouvant être exploité. Comme vu précédemment, les services sont très puissants, trop puissants. Pour les entreprises moyennes, les services de diffusion de publicités donnent une meilleure assurance de la portée et de l'efficacité des publicités que ces entreprises vont produire. Cette même puissance peut aussi être utilisée pour diffuser des idées, des manières de penser. Cette méthode exploite le ciblage extrême proposé par les services de diffusion, de manière à créer plein de publicités extrêmement ciblées, chacune ayant un discours optimisé pour avoir le maximum de chances de faire mouche auprès du public ciblé.

Prenons en exemple le scandale très connu de Facebook Cambridge Analytica. Un petit rafraîchissement rapide de l'affaire : en 2014, Cambridge Analytica (CA) siphonne les données de 80 millions d'utilisateurs de Facebook (principalement des utilisateurs des états-Unis d'Amérique), soi-disant pour une étude scientifique. Pour cela, ils utilisent le système de collecte de données de Facebook, puis ils utilisent ces données pour "conseiller" le parti de Donald Trump sur comment cibler correctement les potentielles personnes qui pourraient voter pour lui. Pour ce faire, ils utilisent les mêmes données pour créer un maximum de publicités extrêmement ciblées pour les 80 M d'utilisateurs. Le résultat : Donald Trump a gagné les élections présidentielles des USA fin 2016. La manipulation du grand public a marché. Il est évident que la victoire de Donald Trump est multifactorielle. L'utilisation des données internes de Facebook, combinée à l'utilisation des systèmes de diffusion de publicité sur le web, de manière à correctement cibler les différents groupes électoraux, n'est qu'une des raisons qui ont permis au parti de Donald Trump de gagner les élections.

Peut-être que l'exemple précédent n'a pas suffi, ou ne plait pas, car pouvant être discuté comme hors sujet, du fait que Cambridge Analytica a utilisé des données internes et non simplement les "données" publiques. Bien, on vous dira que ce n'est pas vraiment le cas. Cambridge Analytica a utilisé les outils de Facebook pour obtenir des données que Facebook possède déjà. Si Cambridge Analytica n'avait pas siphonné les données de Facebook, cela n'aurait pas été un scandale. Cependant Cambridge Analytica pouvait toujours manipuler les élections, sans même avoir besoin des données internes. La seule chose que ses données ont permis, c'est de mettre la lumière sur cette faille immense dans le système. La raison pour laquelle on peut affirmer que Cambridge Analytica pouvait le faire sans, c'est parce que d'autres groupes ont réalisé la même chose. Les dernières élections présidentielles des USA ont subi la même campagne de manipulation, même si c'était à plus petite échelle. Il en est de même pour nos élections en France. Aujourd'hui les politiques utilisent le système pour réaliser leur récolte politique. La différence entre 2016 et

aujourd'hui, c'est qu'aucun de ses groupes n'utilise de donnée "privée", ce n'est donc pas un scandale.

Ces politiques exploitent tous la même faille. Ils n'ont peut-être pas accès direct à ces données, mais le système proposé est si puissant qu'il leur permet quand même d'atteindre leur but. Ici la pub ne sert pas de support au message, mais de support pour gagner une voix car on est sûr de toucher correctement la personne, que le message soit vrai, ou une manipulation de la réalité pour être en accord avec les idées de l'utilisateur. Pas d'importance. Si celui-ci n'utilise que ce site pour obtenir de l'information, alors les publicités du politique qui le touche seront les seules informations qu'il a du candidat lors des votes. Et alors son vote sera peut-être pour ce politique, car n'ayant pas le portrait complet du projet politique du candidat.

On a utilisé l'exemple de la politique, mais cela peut être utilisé par d'autres groupes. Les arnaqueurs en sont un autre exemple parfait, qui pourrait être développé en détail. En soi, ici, les politiques ne réalisent rien d'illégal. Les outils de diffusion de publicité, proposés par ses sites sont légaux (dépendant des régions du monde). En réalité, le problème vient de la consommation de cette même publicité par les utilisateurs. Ici, on est en face d'un problème conjoint avec un autre. Cette autre problème est que ces sites cherchent par tous les moyens à devenir l'unique et seul site des utilisateurs (récréativement, discussions professionnelles ou amicales, source d'information, interaction sociale, etc).

II.1.4 - Les algorithmes de recommandation

Il y a plusieurs systèmes qui sont mis en place par ces sites, pour permettre de maximiser la rétention de leurs utilisateurs. Pousser les utilisateurs à créer des contenus courts, pour que les autres utilisateurs de la plateforme ne soient jamais dans une phase d'ennui. Que parcourir le site ne soit jamais plus loin que 1 clic/mouvement. Que l'utilisateur ne soit jamais arrêté dans l'utilisation du site. Que le site est un retour positif (terme un peu compliqué mais en somme : le site doit être réactif, avoir un minimum de bugs gênants qui viennent entacher l'expérience utilisateur, et donner l'impression que l'utilisateur est au centre du site).

Tous ses "principes" de fonctionnement (en sachant qu'il y en a plein d'autres) possèdent un lien commun: le fameux algorithme de recommandation, la pierre angulaire de tous les géants actuels du Web. Cet algorithme vient lier tous les autres principes entre eux, pour créer un écosystème où l'utilisateur reçoit toujours ce qu'il veut. Cet algorithme possède des règles simples : recommander à l'utilisateur ce qu'il veut voir sans lui demander, mettre en face de l'utilisateur du contenu qui le fera réagir, pour qu'il ne parte pas faire une autre activité. C'est cet algorithme qui est sur-optimisé pour donner les meilleurs résultats. Ces algorithmes sont des monstres d'analyse de données comportementales et de modèles répétitifs ou non. Pour toujours être au top, ils sont souvent mis à jour pour assurer que tout l'écosystème fonctionne. Ces mêmes algorithmes sont aidés par la quantité de données indécente que possèdent les sites, de leurs utilisateurs.

Depuis quelques années, les géants du Web semblent avoir un problème avec leurs algorithmes. Plusieurs organismes dans le monde ont recensé que ces mêmes algorithmes semblent proposer de plus en plus de contenu violent, ce qui fait très fortement réagir. Mais la réalité, c'est que ces algorithmes fonctionnent parfaitement. Il faut bien comprendre qu'il y

a une différence entre nous, utilisateurs du site, qui subissons le fonctionnement de l'algorithme, et le regard d'analyse que l'on peut porter sur le fonctionnement de l'algorithme. Il est évident qu'un algorithme qui met en avant du contenu à caractère suicidaire, en face de personnes susceptibles de commettre le pire, est une très mauvaise idée. Cependant, aux yeux de l'utilisateur, c'est exactement le contenu qu'il voulait voir. L'algorithme a suivi les règles, a proposé ce que voudrait voir l'utilisateur, celui-ci a réagi, il a donc continué. Là est le premier problème des algorithmes de recommandation. Ils enferment les utilisateurs dans des bulles plus ou moins grosses. Ces bulles sont composées de tout le contenu que l'utilisateur va apprécier/réagir. Ici je débute un sujet très important qui sera abordé dans une prochaine partie "les chambres d'échos". Mais pour le moment, on ne va aborder que la partie catégorisation des utilisateurs.

Les algorithmes sont conçus dans deux buts majeurs. Le premier, celui même d'être le lien entre tous les principes qui doivent régir le bon fonctionnement du site. Le deuxième, nourrir le système de récolte de données. Les algorithmes utilisent cette immense base de données pour recommander le bon contenu, mais ils l'agrandissent aussi. Il s'agit d'une boucle sans fin. Le but reste toujours le même: maximiser le profit. Comme pour la récolte de données, les algorithmes ont pour but de mettre les utilisateurs dans les cases. Cette obsession des géants du WEB à vouloir mettre les gens dans des catégories est la raison principale de tous les problèmes. Ce n'est pas la première fois dans l'histoire, que la catégorisation des gens est la raison de beaucoup de problèmes. Mais ici, on est à un autre niveau de catégorisation, qui a pour simple but de faire le plus de profit.

II.1.5 - Réductions du débat et de la discussion au profit de l'aliénation

L'utilisateur doit devenir une sorte d'esclave du site. Que ce soit dans la création de contenu pour celui-ci ou dans l'interaction qu'il entretient avec les autres utilisateurs du site. Il ne doit pas analyser, comprendre, et discuter. L'utilisateur doit voir, lire, réagir. Cette interaction peut prendre deux formes. La première, une banale interaction d'ascenseur. Plusieurs personnes parlent d'un sujet qu'ils connaissent, entre eux, sans frustration et dans un respect commun de la parole de l'autre. La deuxième forme, celle qui fait parler d'elle en permanence, la réaction par colère, ici, on ne discute pas, on s'insulte pour prouver que l'on a raison. Il n'y a plus de débat quand les parties de celui-ci sont obnubilées par une réalité forgée par eux-mêmes. Le but d'un débat est d'arriver à une solution commune, qui convient aux deux (ou plus) parties. Sur ses sites, le débat n'est pas de mise, car une personne qui débat est une personne qui réfléchit à ce qu'elle écrit. Elle n'est donc pas susceptible de réagir à de la publicité et encore moins de dévoiler des informations personnelles. L'algorithme cherche à créer la deuxième. Une réaction forte, c'est assurer une réponse des utilisateurs.

Si ce n'est pas avec une réaction de colère que l'algorithme prendra votre attention, alors ce sera avec d'autres choses. Son but reste le même, vous rendre esclave du site. Une des réactions qui attire le plus les utilisateurs est l'aléatoire. Instagram et TikTok l'avaient très bien compris. Si on ne sait jamais de quoi va parler la prochaine publication, cela incite l'utilisateur à continuer de scroller sans s'arrêter. Car peut-être que la prochaine vidéo sera la bonne. Cela peut paraître ridicule, pourtant ce système fonctionne. Depuis l'émergence de TikTok vers 2016, tous les géants du Web ont réalisé l'intégration de contenu court avec un système de scrolling (YouTube avec ses Shorts, Instagram avec ses Réels, Snapchat, TikTok, etc.). Contenu rapide, qui fait réagir. Si l'utilisateur n'est pas intéressé, il n'a qu'à

scroller, ce qui lui fera apparaître une nouvelle publication. Ce phénomène, de défiler sans jamais s'arrêter en raison de la poussée de dopamine dans le cerveau à chaque nouvelle vidéo, porte un nom : le doom scrolling.

D'autres techniques incluent le contenu aguicheur. Les algorithmes poussent et mettent en avant des vidéos aguicheuses. Cette poussée de vidéos aguicheuses a créé une mode de l'hypersexualisation. Cette mode a fait des ravages et s'inscrit dans une mode plus générale de la recherche de l'attention. C'est un sujet très grave, car rentrant aussi sur le terrain de l'illégalité. Ici n'est pas le document où nous en parlerons, mais il est obligatoire d'ajouter que ce genre de contenu pousse à des comportements très mauvais. La montée de l'addiction au film pornographique chez les jeunes n'est pas déliée de la montée en trombe du contenu aguicheur sur les réseaux. Ce double problème vient encore plus montrer les défauts des algorithmes de recommandations. Le lien commun de toutes ces méthodes : la réaction primaire non réfléchie

Mais cette recherche à la réaction primaire pose un problème. Comme expliqué plus haut, ses sites ont détruit totalement l'espace du débat à l'intérieur d'eux. Ce qui vient poser des problèmes bien plus graves pour nos sociétés.

II.1.6 - La mise en danger des démocraties

Les chambres d'écho sont le fléau qui vient mettre un coup de pied direct au fonctionnement établi de la démocratie. La démocratie est basée sur le principe du débat. Dans une démocratie, on donne le même temps de parole à chaque personne, et toutes les idées posées sur la table sont étudiées pour arriver à un consensus général. Sur les sites des géants du Web, la démocratie n'existe plus depuis quelques années. Comme dit dans la partie précédente, les algorithmes poussent les utilisateurs à la réaction primaire. Mais ils viennent aussi détruire toute forme de débats. C'est ce fameux phénomène des chambres d'écho. Les algorithmes mettent en relation des gens qui possèdent des points communs. Ce ne serait pas un problème si cette catégorisation n'était pas poussée à l'extrême. Chaque bulle est un microcosme de personnes aux idées très proches. Ce groupe discute entre eux, et auto-valide sa méthode de pensée, sans jamais avoir de débat avec un groupe extérieur qui leur permettrait de confronter leurs idées. La seule interaction que l'algorithme créera avec un groupe sera de forcer une confrontation directe avec d'autres groupes, ayant soit des idées différentes et opposées ou même, parfois, les mêmes idées. La réaction à chaud est privilégiée, ce qui crée un champ de bataille où le groupe qui crie le plus fort gagne.

Ceci est la raison pour laquelle les publicités extrêmement ciblées sont un problème pour nos sociétés. Comme vu précédemment, n'importe quel utilisateur de l'outil de diffusion de publicité peut cibler avec une précision chirurgicale quel groupe de personnes recevra la publicité. C'est un problème quand on combine avec un site qui ne repose pas sur des bases de débats. Une publicité d'une politique de gauche pourrait parfaitement toucher des utilisateurs de gauche si correctement mise en place. Comme absorbé par le site, il risque d'accepter les idées proposées par la publicité comme vérité, sans jamais les confronter à d'autres, mais surtout, sans jamais voir la totalité du tableau.

II.2 - Les réponses des différents états

II.2.1 - L'Online Safety Act et d'autres propositions de lois

Depuis 2 à 3 ans, une nouvelle tendance semble avoir été prise par les différents états démocratiques du monde. Entre les retours alarmistes des organisations internationales et les effets des failles du système, les états semblent prendre de plus en plus de décisions hâtives aux conséquences graves pour les utilisateurs. Dans l'Union européenne, le RGPD est un parfait exemple de texte de lois réussi (même s'il n'est pas sans faille exploitable), permettant à n'importe quel habitant de l'UE de faire valoir son droit d'anonymat sur le Web. Le RGPD protège l'utilisateur du Web de l'utilisation de ses données comme monnaie d'échange ou outil de renseignement. Cependant, cette loi ne vient que donner un droit de réponse à l'utilisateur. Ici le RGPD est un ensemble de règles permettant de prévenir l'utilisateur que ses données seront collectées, mais n'empêche pas les entreprises de le faire. Si l'utilisateur tient à retirer ses données des bases des courtiers en données, alors l'utilisateur devra réaliser une démarche auprès du site pour faire valoir ses droits, ou au pire, aller en justice. Pour pouvoir régler ce problème du RGPD, l'UE réfléchit sur 2 autres textes qui permettent de réellement empêcher la collecte de données.

Le RGPD fut l'un des premiers textes à garantir que tout utilisateur du Web puisse demander de retourner dans l'anonymat auprès de toutes les entreprises du secteur. Ce texte fut tellement avant-gardiste qu'il a démarré, à lui tout seul, la création de textes similaires dans d'autres états, comme en Inde (**DPDPA**) ou au Japon (**LPPI**). Cependant, tous les états du monde n'ont pas pris la décision de suivre les idées du RGPD.

En 2023 au Royaume-Uni, une proposition de loi se voit pousser au sommet des discussions parlementaires, l'Only Safety Act (**OSA**). Cette loi vient plutôt s'inscrire dans une lignée préventive. Au lieu de donner des droits de réponse aux utilisateurs du Web, quant à la protection de leurs données, l'OSA vient exiger, auprès des différents géants du Web, des règles à respecter. Dans l'idée, si l'OSA exigeait des entreprises de ne pas récolter des données privées, de réaliser de la publicité ciblée et toute autre pratique pouvant mettre en danger l'utilisateur, alors cette loi serait l'une des premières à garantir une sécurité pour les utilisateurs. Mais malheureusement, l'OSA n'est pas ce texte. Dans son introduction, l'OSA se veut être un texte qui rend responsables les sites de la sécurité des utilisateurs du site. Le texte est en réalité une liste de toutes les choses que les sites ne doivent pas faire, s'ils veulent éviter des répercussions juridiques. Il n'y a aucune exigence sur le fait de ne pas collecter de données personnelles, aucune protection des utilisateurs sur la publicité ciblée. Il en va de même pour les algorithmes, aucune limitation. En réalité, les sites sont libres de faire ce qu'ils veulent. La seule réelle chose que les sites doivent faire, c'est s'assurer que tous les utilisateurs de leurs sites sont dans la tranche d'âge exigée par l'OSA (tranche d'âge définie par une liste cumulative. Un site pouvant proposer du contenu violent se doit de vérifier que chaque utilisateur a 15 ans et plus, même si le site ne produit pas ce contenu, mais que les utilisateurs peuvent le faire, alors que cela est interdit par le site sous peine de sanction. Le site doit tout de même vérifier l'âge des utilisateurs.) On pourrait rajouter que tout site qui parle de maladie mentale doit assurer que chaque utilisateur du site a 18 ans ou plus. Pour faire simple, tout site permettant d'écrire du texte (forum, réseaux sociaux et autres) est inclus dans la vérification d'âge.

Ce type de loi irréaliste englobant une gigantesque partie des sites du Web semble devenir de plus en plus en vogue. Ici, ces lois ne cherchent pas à réellement protéger l'utilisateur, mais à réduire l'accès au site. Si moins de personnes peuvent y accéder, alors forcément cela règle le problème, non ? Il est évident que ces lois semblent avoir été rapidement écrites, sans réelle pensée à comment réaliser une loi fonctionnelle et applicable.

Après le retour d'enquête d'Amnesty International sur les dysfonctionnements des algorithmes de recommandation de TikTok, la France à mis en place une commission générale d'étude, dans le but d'arriver à écrire un texte de loi solide qui permettrait de protéger les utilisateurs du site, et non de simplement donner un droit de réponse. Pour ce faire, la commission générale a demandé de l'aide à différents influenceurs du Web (Hugodecrypte pour ne citer que lui). Plusieurs discussions ont eu lieu, avec certaines qui ont très vite fini en cours de récréation pour des influenceurs-voleurs, et d'autres masculinistes toxiques qui faisaient (et font toujours) des ravages sur les réseaux comme TikTok et YouTube. Après 6 mois de discussion et de révision, le prévisionnel de la loi fut dévoilé. Et c'est un fiasco. Premier point de décrédibilisation de cette loi, elle ne vise que TikTok. Nous ne pensons pas avoir besoin d'expliquer en quoi TikTok n'est pas le seul site à utiliser des algorithmes de recommandation douteux, et à récolter des données personnelles pour permettre le ciblage publicitaire. Ce n'est pas le seul problème de cette loi. Comme pour l'OSA, cette loi exige de TikTok une vérification de l'âge des utilisateurs pour attester d'une sécurité. Ici, pas de demande à TikTok, de changer ses pratiques, seulement de restreindre l'accès. De plus, la loi stipule un couvre-feu des enfants (ce couvre-feu devant être renforcé par les parents) dans le cas de l'utilisation des réseaux sociaux après 19 heures (à savoir que les parents sont susceptibles de subir une amende, s'ils n'appliquent pas ce couvre-feu). Ce couvre-feu, comme pour la restriction d'accès, s'applique pour toute personne en dessous de 18 ans. Le seul bon changement notable que cette loi tient à appliquer est le changement de l'âge minimum d'utilisation des sites comme TikTok (en somme les réseaux sociaux) à plus de 15 ans.

Cette tendance à vouloir restreindre l'accès aux sites Web est le nouveau problème auquel les utilisateurs du Web ont à faire face. Ici, ce ne sont pas les sites qui tentent de vous faire du mal (métaphoriquement), mais votre État.

II.2.2 - Réduire l'anonymat, une fausse bonne idée

Par quel moyen ces lois ont-elles demandé d'assurer l'âge des utilisateurs ? Avec une image recto-verso de la carte d'identité ou du permis de conduire. En France, le texte oblige la suppression de ces données sous 24h. De plus, les sites seront tenus responsables de la mauvaise utilisation de ces données. Dans le cadre de la loi, elles ne peuvent utiliser leurs données que comme un outil de certification de l'âge et non de données réutilisables. Chaque site se doit de s'occuper de recevoir, traiter, et supprimer les données, sans jamais pouvoir déléguer le travail à une autre entreprise. En France, la loi a eu le bon sens de ne pas permettre au site d'utiliser ces données comme un autre outil. Au Royaume-Uni, c'est un autre problème. Non seulement on perd notre anonymat auprès des sites, mais de plus, les Britanniques se voient à risque de voir leurs données exploitées par ces mêmes entreprises. À contrario de la loi française, l'OSA permet la conservation des données utilisateur (pas indéfiniment cependant). De plus, l'entreprise qui se doit de vérifier l'âge peut déléguer le travail de traitement et stockage/destruction des données. C'est un point

évidemment problématique, qui, seulement 8 mois après son implémentation au Royaume-Uni, est déjà responsable d'une des plus grandes fuites de données privées extrêmement sensibles du 21e siècle.

De plus, on est en droit de se demander si cette réduction de notre anonymat est une bonne chose. Même si les lois qui exigent cette vérification assurent que cela permettra de réduire l'impact et l'influence néfaste des réseaux sociaux sur les jeunes. Cela reste à relativiser. Il est évident que si moins de personnes ont accès aux sites, alors moins de personnes subiront les effets néfastes de ces mêmes sites. Cependant, ça ne règle pas les problèmes de départs. Ici les sites n'ont pas d'obligation de changer leurs pratiques, seulement d'implémenter une interdiction d'accès qui leur est avantageuse. Comme vu précédemment, les sites utilisent leurs fonctionnalités comme outils de récolte de données, les états exigent les sites à récolter les données privées les plus sensibles pour pouvoir exister. Il légalise la récolte de données sensibles pour une prétendue protection des enfants. En somme, ces lois nous demandent de sacrifier notre anonymat, pour aucun changement concret. Rien n'a changé, tout est pareil, sauf une chose. On doit donner plus d'informations sur nous. Il en va de même pour les vérifications par carte bancaire (les paiements à 0,00 € donnent tout autant d'informations, voire parfois plus, qu'une carte d'identité).

De plus, cette perte d'anonymat risque d'apporter bien plus de problèmes qu'elle n'en règle. Entre des potentielles fuites de données (exemple de Discord, où des dizaines de millions d'utilisateurs ont vu leurs cartes d'identité fuiter sur le Web), ou encore les risques de doxxing (pratique qui consiste à récolter des données privées sensibles d'une personne, puis de s'en servir contre lui. Soit en les publiant à la vue de tous, ou en l'utilisant comme levier pour obtenir des faveurs). Il y a 15 ans, on demandait aux utilisateurs d'internet de ne jamais diffuser de données personnelles. Aujourd'hui, ce sont les états eux-mêmes qui nous obligent à le faire, pour obtenir une soi-disant sécurité. Des entreprises ont tenté de le faire par le passé, et ça a très mal fini. Des forums de discussion, qui demandent de simplement donner leurs nom et prénom réels, ont permis à des groupes mal intentionnés, de doxxer des gens et d'obtenir des faveurs. Les technologies du WWW ont toujours fonctionné sur le principe de l'anonymat. Mais maintenant, nos états souhaitent jeter par la fenêtre l'essence même du Web. Le Web n'a pas besoin de voir ses utilisateurs, de diffuser leurs données personnelles sensibles pour une prétendue sécurité.

III - Tech literacy : vers une nouvelle ère du numérique

III.1 - La nécessité d'un numérique plus transparent

D'après infosecinstitute, près de 85% des hacks sont causés par une erreur humaine. Par exemple, le hack du Bundestag Allemand, en 2015, a été causé par un simple mail de phishing [22]. La majorité des vecteurs d'attaque les plus populaires, comme le hack au faux service client, le hack du menu "Run" Windows ou plus récemment des injections d'instructions malicieuses pour tromper les IAs dans les descriptions de vidéos youtube ont tous un point en commun : ils dépendent d'une erreur humaine et sont souvent ineffectives contre des personnes habituées à la technologie. Quels chemins pouvons nous entreprendre pour pallier ce problème?

On peut remarquer une tendance vers la simplification du numérique, telle que la simplifications des applications, comme le déplacement de la barre de recherche du playstore vers son petit icône dédié dans la barre d'outil au lieu de l'avoir au centre de l'attention en haut de l'écran, poussant vers une utilisation passive de l'application et promouvant une action de scroll, ou bien l'obfuscation volontaire d'applications et de jeux, les rendant inutilement hostiles à la modification ou modding tel que les environnements always online pour du logiciel qui n'en dépend pas, comme Star Wars: Hunter ou XDefiant[23], forçant une connection à un serveur contrôlé par la compagnie du jeu pour simplement lancer le jeu, poussant à la consommation de nouveaux titres souvent très peu originels comme la série des jeux FIFA d'activision dès que la compagnie décide que le jeu n'est plus assez lucratif[24] sans aucun partage d'exécutables de serveurs privés, malgré que le produit rendu volontairement inutilisable soit toujours techniquement jouable si la communauté décide d'héberger ses propres serveurs. Cette hostilité calculée, des fois résultante d'évolutions cherchant à rediriger l'utilisateur vers une utilisation spécifique d'un produit, comme un nouveau jeu avec de nouvelles microtransactions ou bien la barre de recherche du playstore étant déplacée vers un endroit incitant le scroll du playstore et le visionnage de contenus sponsorisés, ou bien la barre de recherche de windows étant modifiée pour proposer des recherches sur le web avec bing au lieu d'afficher des résultats de fichiers locaux trouvés, sont nuisibles pour l'utilisation fluide d'un outil. L'utilisateur veut utiliser le playstore pour installer une application dont il a entendu parler, pas découvrir de nouveaux gadgets sponsorisés. L'utilisateur veut utiliser la barre de recherche de l'ordinateur pour trouver un fichier qu'il a perdu dans son arborescence de fichiers, pas rechercher "spreadsheet q4 2024" sur bing. L'utilisateur veut jouer à son jeu favori qu'il a payé, pas se retrouver avec un message "Serveur non trouvé". Plusieurs alternatives existent déjà, telles que Linux, Librewolf, FDroid, Aurora Store, mais la transition est difficile en raison d'un écosystème volontairement hostile, tel que google mettant en place des restrictions envers le sideloading[25] (installation d'une application à travers d'une source non officielle), une complexité apparente, ou simplement par un manque de connaissances. Même si des distributions Linux sont faites de plus en plus facile d'utilisation, et que des utilisateurs mécontents avec le contenu des mises à jour de Windows aient décidés de passer à Linux en grand nombre, Windows contrôle toujours près de 95% du marché des systèmes d'exploitations d'appareils personnels d'après la Steam Hardware Survey[26] de q4 2025. Une adoption de ces alternatives libres et ouvertes comme premier pas avec la tech serait un excellent moyen d'améliorer les compétences en informatique de la population et donc d'améliorer leur résilience aux techniques de manipulation courantes. L'objectif serait de rendre l'utilisateur assez bien informé sur le fonctionnement de l'informatique pour qu'il devienne résilient aux arnaques afin de rendre ces techniques d'hameçonnage peu viables. En effet, le simple fait de comprendre le principe derrière l'encryption, les adresses mail, l'authentification à double facteur et les tokens d'accès permettrait de stopper la majorité des arnaques les plus courantes tels que les mots de passe faciles à deviner ou réutilisés, les faux mails de phishing ou bien des faux portails de connection permettrait de rendre le phishing une activité tellement complexe que lire un script à des mamies à une échelle industrielle ne serait plus viable.

III.2 - Innovations et applications de technologies protectrices

Plusieurs technologies ont déjà été développées afin d'améliorer la résilience aux attaques des systèmes informatiques tels que l'encryption de bout à bout, où les deux ordinateurs communiquent en messages codés, rendant les attaques de man in the middle où un individu malicieux peut intercepter les paquets de communication et facilement les lire inefficace. Cependant, avec les progrès en technologies quantiques, ces algorithmes de chiffrement sur lesquels reposent ces technologies sont en danger, tel que le sha256. Mais, de nouveaux algorithmes résistants existent déjà, tel que la série CRYSTALS, ML-KEM, ML-DSA ou SLH-DSA du NIST[27] (National Institute of Standards and Technology), qui font partie de candidats de nouvelles spécifications d'algorithmes de chiffrements, que le NIST suggère fortement d'implémenter au plus vite. Un autre danger pour le numérique est la sur-dépendance de services clés, tels que les services de DNS (serveur de nom de domaine), des services de protection tels que les antivirus opérant avec la même priorité que le noyau du système d'exploitation ou des autorités gérant le déploiement de certificats d'authentification des sites web. On peut noter deux accidents qui ont grandement affecté le monde moderne, causés par un mauvais fonctionnement de ces systèmes, tel que la mise à jour défaillante de crowdstrike, un antivirus kernel level qui a bloqué dans une boucle de redémarrage, où les ordinateurs cessaient de fonctionner dès leur démarrage, les systèmes informatique de la majorité des grands aéroports dans le monde, ou bien le dysfonctionnement d'un serveur de Cloudflare, un service de protection contre le DDOS (attaque par surcharge de servers avec des paquets provenant de multiples machines coordonnées) et peu après d'AWS un service hébergeant énormément de services clés, qui a causé une grande partie du web à cesser de fonctionner. La plupart de ces technologies protectrices comme l'end-to-end encryption ou le chiffrement post-quantique sont des fois implémentées ou non; on peut noter une bataille sur deux fronts; ou d'un côté certains systèmes sont cruciaux à un numérique stable et sûr comme les algorithmes d'encryption et la décentralisation des services critiques, et d'un autre côté on a des états qui poussent vers un partage des clés d'encryption systématique avec les autorités locales comme la proposition de régulation des communications numériques de CSAM en europe, ou le actuel Child Safety Act en Grande Bretagne, qui a lui par ailleurs causé une brèche de données massive[28] de cartes d'identités, d'adresses et de numéros de téléphone de milliers de mineurs.

III.3 - Entreprises : entre opportunisme et réel engagement

Plusieurs entreprises promeuvent leur position sur le respect de la vie privée tel que Meta[29] et Whatsapp[30], Telegram, ou bien encore Apple[31]. Cependant, ces positions sont des fois purement commerciales, et ne sont pas très efficaces en réalité, comme whatsapp qui collecte et partage une grande collection de métadonnées sur ses utilisateurs telles que les heures d'activité, Telegram qui a l'end to end encryption comme option désactivée par défaut, et Apple qui assume dans leur page de termes et conditions être capable de partager des données sensibles avec des autorités gouvernementales. Ces failles de sécurité malgré un marketing poussant vers une idée d'une vie privée respectée pourraient simplement être à l'origine d'une implémentation bâclée ou bien être à l'origine de privacy washing, une pratique ou un produit est vendu comme sûr mais en fait contient des failles de sécurité assez aberrantes. Par exemple, le hack de photos explicites de célébrités en 2014[32], dû à des mots de passe réutilisés et du téléversement automatique des images

d’un iphone vers les serveurs icloud d’Apple. Est ce que toutes nos photos ont vraiment besoin d'être téléversées dans le cloud automatiquement par défaut?

III.4 - L’utilisateur, comme acteur de sa souveraineté numérique

L’utilisateur, comme maillon faible de la chaîne de sécurité, mais cependant indispensable au numérique, est le centre de l’attention des malfaisants. Donc, naturellement, renforcer ce maillon est le chemin le plus direct en faveur d’un numérique plus sûr. Mais, cernés de tous les côtés, l’utilisateur semble enfermé dans un bocal. Les megacorps veulent maximiser la rétention de leurs utilisateurs et extraire un maximum de données afin de les monétiser, sans hésitation ou scrupule. D’un autre côté, les gouvernements tentent de faire passer des lois forçant la désanonymisation des communications tout en gardant leurs communications opaques, tel que marqué en pleines lettres dans une proposition de loi européenne, section 12a[33]. Ces barricades bloquent l’utilisateur dans un bocal de consommation sans arrière pensée ou connaissance du fonctionnement interne du web. Pour s’en échapper, l’utilisateur doit donc choisir de son plein gré une alternative et l'étudier, comprendre son fonctionnement. De plus, peut être qu'avec assez de voix, les états pourraient s'activer, créer et imposer des lois anti monopole, utiliser du logiciel ouvert dès le plus jeune âge des citoyens et promouvoir un utilisateur savant envers le fonctionnement du numérique, résistant à la majorité des arnaques les plus communes.

Bibliographie

- Bruno Patino, *La civilisation du poisson rouge*, Grasset, 2019

- Jean-Louis Missika et Henri Verdier, *Le business de la haine*, Liberté de l'esprit, Clamann Lévy, 2022

- Valérie SEGOND, *Des données personnelles très convoitées*, Le Monde, 29 mai 2017, https://www.lemonde.fr/economie/article/2017/05/28/des-donnees-personnelles-tres-convoitees_5135092_3234.html

- Mary Jane Kwok Choon, *Publiquement privé*, OpenEdition Journals, Communication,Vol.35/1, 2018, https://journals.openedition.org/communication/7571

- Valérie FORTIER, *Nos données personnelles : un marché convoité*, CScience, 28 avril 2021, https://www.cscience.ca/nos-donnees-personnelles-un-marche-convoite/

- Mathilde GUILBAUD, *Vos données personnelles valent de l'or, et cette entreprise propose de vous les acheter*, l'édition du soir, Ouest-France, 19 mai 2025, https://www.ouest-france.fr/leditiondusoir/2025-05-19/vos-donnees-personnelles-valent-de-l-or-et-cette-entreprise-propose-de-vous-les-acheter-4ab4de7c-d021-4982-b56f-59897ffc40e8

- Blog de l'universiter de Bordeaux https://blogacabdx.ac-bordeaux.fr/unum64/2020/04/29/quelles-donnees-personnelles-sont-les-plus-recherchees/

- Courtier en données - Numéro de version : 227541912, date : 24 juillet 2025 à 15:32

- Économie de l'attention - Numéro de version : 227642792, date : 28 juillet 2025 à 12:57

- Vie privée et informatique - Numéro de version : 229926109, date : 20 octobre 2025 00:39

- Scandale Facebook-Cambridge Analytica - Numéro de version : 230122450, date : 27 octobre 2025 17:48

- Comprendre le RGPD, groupement d'articles sur les sujets du RGPD

- *Cookies et traceurs : que dit la loi ?*, 29 septembre 2020

- *France : TikTok still steering vulnerable children and young people towards depressive and suicidal content*, Rapport d'enqête, 20 octobre 2025, Amnesty International

- *Online Safety Act*, Texte officiel expliquant le but et les aboutissants de cette futur loi

- Cookie walls : la CNIL publie des premiers critères d'évaluation,CNIL https://www.cnil.fr/fr/cookie-walls-la-cnil-publie-des-premiers-criteres-devaluation

- https://data.europa.eu/fr/publications/open-data-impact#:~:text=La%20taille%20du%20marché%20des,le%20secteur%20des%20données%20ouvertes.

- Elijah Greisz† ,Transparency Without Teeth: An Empirical Understanding of Data Broker Regulation,university of chicago, https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=6434&context=uclrev&utm_

- Comment se protéger ?,CNIL https://www.cnil.fr/fr/cookies-et-autres-traceurs/comment-se-proteger

- Cookie walls : la CNIL publie des premiers critères d'évaluation,CNIL https://www.cnil.fr/fr/cookies-et-autres-traceurs/comment-se-proteger/maitriser-votre-navigateur

- Cookies et traceurs : que dit la loi ?,CNIL https://www.cnil.fr/fr/cookies-et-autres-traceurs/que-dit-la-loi

- https://www.infosecinstitute.com/

- https://stopkillinggames.wiki.gg/wiki/Dead_game_list - Numéro de version : 875, date : 27 février 2026 12:20

- Shaun Prescott,*Spectre Divide and its studio are shutting down after just six months: 'The industry is in a tough spot right now*,PC GAMER,yahoo tech,13 mars 2025,https://tech.yahoo.com/general/articles/spectre-divide-studio-shutting-down-020726939.html

- Suzanne Frey,*A new layer of security for certified Android devices*,Android developers blog,25 Aout 2025, https://android-developers.googleblog.com/2025/08/elevating-android-security.html

- Steam,Sondage sur le matériel et les logiciels : february 2026,Février 2026,https://store.steampowered.com/hwsurvey/Steam-Hardware-Software-Survey-Welcome-to-Steam

- Csrc,Post-Quantum Cryptography, 11 décembre 2025,https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

- Discord,Update on a Security Incident Involving Third-Party Customer Service,9 octobre 2025, https://discord.com/press-releases/update-on-security-incident-involving-third-party-customer-service

- Facebook,Qu'est-ce que la Politique de confidentialité et que couvre-t-elle ?,politique de confidentialité,https://www.facebook.com/privacy/policy/,16 décembre 2025

- Whatsapp,Est-ce que WhatsApp recueille ou vend vos données ?,https://faq.whatsapp.com/2779769622225319

- Apple,Apple Privacy Policy,30 juillet 2025,https://www.apple.com/legal/privacy/en-ww/

- https://en.wikipedia.org/wiki/2014_celebrity_nude_photo_leak Numéro de version : 1295749019, date : 15 juin 2025 16:34

- Council of the European Union ,Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse ,6 novembre 2025, https://cdn.netzpolitik.org/wp-upload/2025/11/2025-11-06_Council_Presidency_LEWP_CSA-R_Presidency-compromise-texts_14092.pdf

- https://fr.wikipedia.org/wiki/Cookie_(informatique) Numéro de version : 234365834, date : 23 mars 2026 12:06

- Twilio,4 types de données clients à exploiter pour les entreprises,

- Cookie,CNIL https://www.cnil.fr/fr/definition/cookie

- Acxiom,pdf,*REACH OVER 2.5 BILLION OF THE WORLD'S MARKETABLE CONSUMERS*,https://marketing.acxiom.com/rs/982-LRE-196/images/Acxiom%20Global%20Data.pdf
-
- https://fr.wikipedia.org/wiki/Acxiom Numéro de version : 234275298, date : 21 mars 2026 04:32

- Matthieu Delacharlery,*"Ils en savent autant sur vous qu'un ami proche" : que sont les "data brokers", qui traquent et revendent vos données ?*,TF1INFO,TF1,30 janvier 2025,https://www.tf1info.fr/high-tech/vie-privee-sur-internet-que-sont-les-data-brokers-qui-brassent-des-milliards-grace-a-vos-donnees-2347615.html

- Antoine Bouchet,En interdisant les bloqueurs de publicité, YouTube est-il hors la loi ?,Le Figaro économie,Le Figaro,3 novembre 2023, https://www.lefigaro.fr/conjoncture/en-interdisant-les-bloqueurs-de-publicite-youtube-est-il-hors-la-loi-20231103