N° spécial campagne

Contrastes

bpost
PB-PP
BELGIE(N) - BELGIQUE

► N° 188 ▪ Bimestriel ▪ Septembre-octobre 2018 ◄

Equipes Populaires

SURFEZ COUVERTS!

Une campagne de sensibilisation des Equipes Populaires

www.equipespopulaires.be

Avec le soutien de

FÉDÉRATION WALLONIE-BRUXELLES

Bureau de dépôt : 5000 Namur mail. N° d'agréation : P 204078 - Equipes Populaires, rue du Lombard,8 5000 Namur

2018, L'ODYSSÉE DES GAFA*

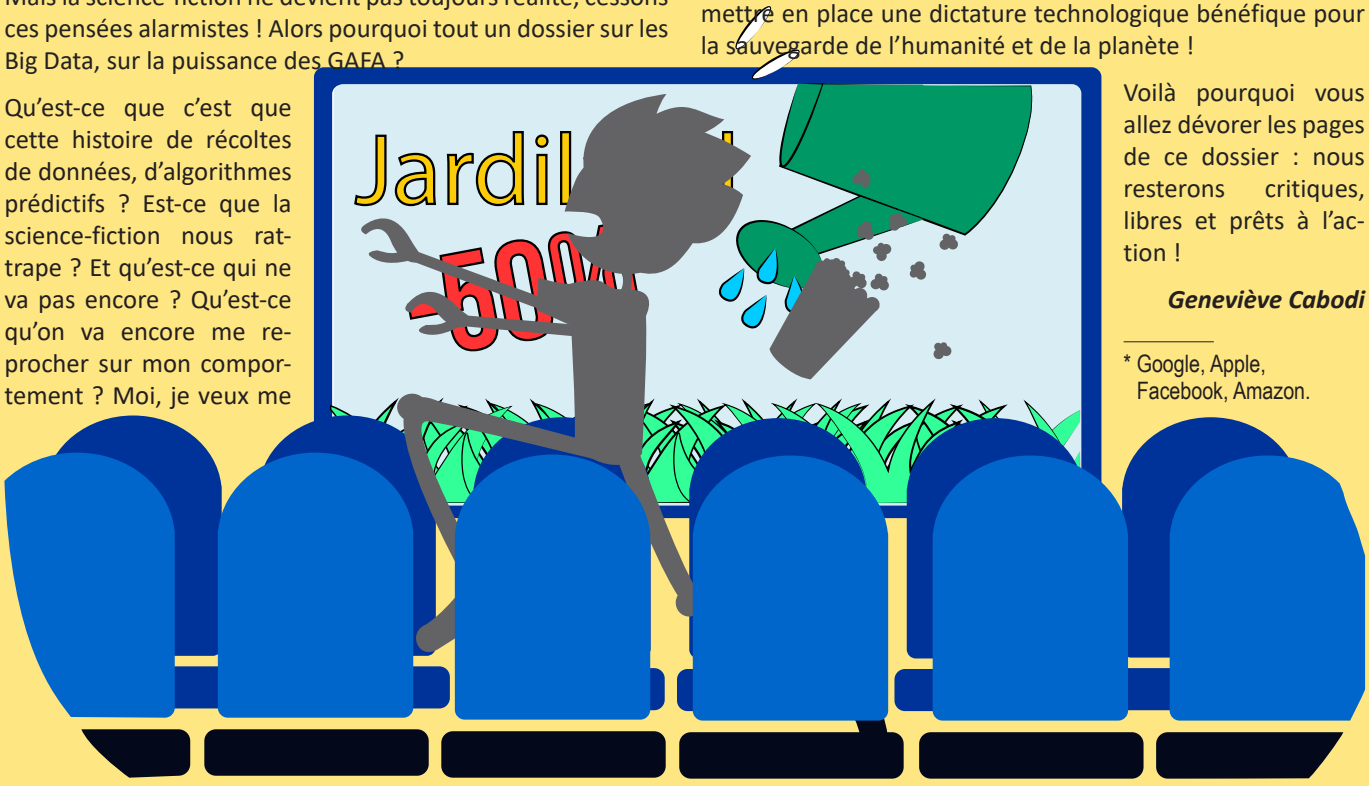
En 1978, j'avais 14 ans quand j'ai vu pour la première fois au cinéma le film « 2001 l'Odyssée de l'espace » de Stanley Kubrick. J'ai très clairement en tête la scène où un des protagonistes se trouve dans une station spatiale gigantesque et où il téléphone à sa fille pour lui souhaiter bon anniversaire. Ce coup de fil s'apparente aujourd'hui à un échange sur Skype ou sur Whatsapp, rien de plus anodin de nos jours. Mais à cette (lointaine) époque, sur mon siège de cinéma, je me souviens très clairement de ma pensée : « OK pour la station spatiale gigantesque, OK pour le voyage habité vers Jupiter, OK pour l'hibernation, OK pour une pierre noire qui circule dans l'espace infini, mais utiliser un écran et un micro sans fil pour téléphoner depuis l'espace… c'est du grand n'importe quoi, ça n'arrivera jamais ! ». 25 ans plus tard, Skype fait son apparition.

Et je suis donc devenue une grande fan de science-fiction. En 2002, je ne rate pas la sortie du film « Minority Report ». Ce coup-ci c'est Steven Spielberg qui s'y colle. L'action se passe en 2054. À nouveau une scène m'interpelle : le héros est tracé grâce à la reconnaissance faciale et plus spécifiquement la reconnaissance oculaire. Quand il rentre dans une grande surface, il est accueilli par un écran qui affiche son nom, lui souhaite la bienvenue et lui propose une promotion sur des achats potentiellement intéressants pour lui par rapport à ses emplettes précédentes ! 2002 ! Il y a 16 ans de cela, et cette technologie existe déjà dans certaines parties du monde !

Mais la science-fiction ne devient pas toujours réalité, cessons ces pensées alarmistes ! Alors pourquoi tout un dossier sur les Big Data, sur la puissance des GAFA ?

Qu'est-ce que c'est que cette histoire de récoltes de données, d'algorithmes prédictifs ? Est-ce que la science-fiction nous rattrape ? Et qu'est-ce qui ne va pas encore ? Qu'est-ce qu'on va encore me reprocher sur mon comportement ? Moi, je veux me connecter sur mon smartphone et trouver un resto italien ouvert à Virton le dimanche soir sans me prendre la tête. Et si en plus ce resto a été liké par mes amis via Facebook, tant mieux ! Je veux alléger mon portefeuille et n'avoir qu'une carte à puce : identité, banque, carte de fidélité, parc à containers, mutuelle ! Quoique, une carte c'est encore de trop, puisque je peux presque tout gérer via mon smartphone ! Je n'ai rien à cacher ! J'ai même tout à y gagner : je reçois des notifications de promotions sur mes achats potentiels, des notifications sur des rencontres probables dans mon quartier, des propositions de divertissements qui correspondent à mes envies ! Les géants du web se font des montagnes d'argent sur mon dos ? Je veux qu'on me le prouve !

Il y a quelques mois, mon fils m'a offert la trilogie « Fondation », écrite par Isaac Asimov en 1942. Le héros invente une nouvelle science, la psychohistoire, fondée sur la loi des grands nombres et le calcul des probabilités qui permet de « prévoir l'avenir ». Et finalement, l'avenir de l'humanité est prise en main par des robots car nous, humains, sommes considérés dans ce roman comme des enfants qui jouent, insouciants des conséquences de leurs actes ! Dans la même veine, j'ai récemment assisté à une conférence donnée par un professeur de mathématique de l'ULB qui travaille avec son équipe sur les algorithmes prédictifs basés sur l'analyse de récolte de données individuelles. Ce discours de l'Homme incapable de se gérer collectivement était le sien ! Pour lui, la seule solution était de mettre en place une dictature technologique bénéfique pour la sauvegarde de l'humanité et de la planète !



Voilà pourquoi vous allez dévorer les pages de ce dossier : nous resterons critiques, libres et prêts à l'action !

Geneviève Cabodi

* Google, Apple, Facebook, Amazon.

Equipe de rédaction : *Monique Van Dieren, Claudia Benedetto, Guillaume Lohest*
Rédactrice en chef : *Monique Van Dieren* - **Mise en page :** *Hassan Govahian*
Editeur responsable : *Paul Blanjean*, 8, rue du Lombard 5000 - Namur - Tél : 081/73.40.86
secretariat@equipespopulaires.be **Prix** au n° : 2 € - **Pour s'abonner** (Contrastes + Fourmilière) : Versez 15 €
au compte BE46 7865 7139 3436 des Equipes Populaires, avec la mention : "Abonnement à Contrastes" + votre nom

BLACK MIRROR POWER

Aujourd'hui comme tous les autres jours, vous vous réveillerez, jetterez peut-être un œil à votre partenaire, puis, vous likerez, tweeterez, retweeterez, posterez, vous scruterez votre fil d'actualité pour vous assurer que vous n'en aurez pas perdu une miette. Ensuite, vous recommencerez plus de 26fois * dans la journée. Le black mirror ** toujours à portée de main, vous surferez sur la vaste étendue, cet océan de contenus, presque surréaliste puisque infini. Vous y rechercherez des infos mais en même temps, vous y laisserez les vôtres parfois même sans le savoir. Qui exploite vos traces sur le net et à quelles fins ?

Comme plus de 4 milliards[1] d'individus, nous alimentons un monde parallèle si addictif. Nous y laissons des traces invisibles à l'œil nu, çà et là un peu de nous, de notre caractère, un peu de notre image retravaillée. Toujours avoir le smile, toujours montrer le meilleur profil, c'est grisant, c'est kiffant de se mettre au centre de la scène, de jouer à la star. On ne peut pas résister à l'appel de la reconnaissance, de la valorisation de soi quitte à y laisser des plumes.

Nous avons tous en commun, internautes, citoyens du monde, des partenaires qui nous connaissent mieux que notre petite amie, petit copain, notre meilleur ami(e), nos parents, nos enfants : Google, Facebook, Instagram, Twitter, Apple, Messenger, WhatsApp, Snapchat… nous les connaissons tous. Ils font partie de nos vies depuis un certain temps maintenant, nous les connaissons mais pas autant qu'eux nous connaissent. Devant eux, nous n'avons pas hésité à nous mettre à nu, parfois même sans être consentants, sans en être véritablement

* Etude menée par le cabinet d'audit Deloitte sur les Français et leur smartphone, publiée le 16 janvier 2017.

** Littéralement « miroir noir », titre d'une série britannique à succès qui explore les conséquences de l'invasion de nos vies par la technologie. « *Le "miroir noir", c'est ce que vous trouvez sur tous les murs, dans tous les bureaux, au creux de toutes les mains : l'écran froid et brillant d'une télévision, d'un ordinateur ou d'un smartphone* », Charlie Brooker, créateur de la série.

conscients. Nous nous sommes dévêtus sans une once d'hésitation, nous leur avons fait confiance à la première rencontre, acceptant de leur donner accès à notre intimité, à nos habitudes de vie, à nos secrets les plus enfouis. Cette confiance, peut-être la leur avons-nous accordée si facilement parce que ces êtres virtuels nous paraissent irréels, dématérialisés ou aussi et surtout parce que leurs services sont gratuits.

Internet, une utopie libertaire

Au début de l'ère numérique, la création d'Internet a inspiré le mouvement hippie à San Francisco, mû par un idéal libertaire ; gommer les inégalités, plus de noirs, plus de métisses, plus de blancs, plus de vieux ni de jeunes, plus de riches ni de pauvres. Tout le monde aurait accès à ce flux continu d'information. Mais à la fin des années septante, c'est la douche froide, les premières start-up investissent la Silicon Valley et les grands idéaux poétiques résistent difficilement au réalisme du business.
Le business… Cette vision a fini par prendre une place considérable pour ne pas dire toute la place. Aujourd'hui, le modèle économique sur lequel reposent Google et Facebook pour ne citer qu'eux, se base sur les revenus publicitaires. A titre d'exemple, au quatrième trimestre 2017, les recettes publicitaires de Facebook ont pesé pour 98,5% du chiffre d'affaires total de l'entreprise[2]. Ces derniers ne vendent pas les données personnelles mais ils mettent en relation les annonceurs avec leur public cible et c'est cela qu'ils facturent. C'est le prix à payer, le prix qu'on a tous accepté de payer pour nous voir ouvrir les portes de ce paradis de désirs. Pourtant, d'emblée, on sentait que le deal était bancal. Comment était-ce possible que l'on puisse jouir de toutes ces merveilles sans débourser un seul cent ? On ne voulait pas voir la réalité en face ou on ne voulait pas nous la montrer. Tous enfouis dans un déni profond, nous avons profité chaque jour de notre existence à commenter, shazamer, spotifyer. Nous avons plongé notre main dans ce sac rempli de bonbons « gratuits » qu'on pouvait consommer sans modération jusqu'à la boulimie, jusqu'à abandonner une partie de nous-mêmes.

Le système est bien rôdé, on crée des besoins, de nouveaux usages qui deviennent des mœurs, des automatismes. Et dire qu'il y a tout juste vingt ans, on jouait à *snake*, au serpent sur le fameux Nokia 3310 ! Et il y a dix ans, Facebook n'existait pas.

Like Addict

Les notifications activent dans notre cerveau de la dopamine, hormone qui nous procure une sensation de plaisir activé par un système de récompense-renforcement. Vous vous souvenez de ce bon vieux Pavlov et de son expérience avec son chien ? Je vous laisse le googliser. Smileys, émoticônes, ces frimousses jaunes qui rythment nos échanges traduisent l'immédiateté à laquelle nous sommes tous, à différents degrés, voués. Plus besoin de texte, une image vaut toujours mieux qu'un long discours, d'autant plus dans une danse aussi frénétique que celle des « social media », les réseaux sociaux.

Âge, genre, orientations sexuelles, adresse IP, lieu de résidence, problèmes de santé, préférences idéologiques… Toutes ces informations sont précieuses et ont une valeur marchande. Serions-nous des espèces d'esclaves, de par nos activités sur la toile, à la solde des GAFAM ? Cet acronyme rassemble le « top five » des entreprises qui se partagent 95% de la part publicitaire générée par le marché des données personnelles : Google, Apple, Facebook, Amazon et Microsoft. Précisons qu'une grande partie du revenu de Google et Facebook est issue de revenus publicitaires : 85,6% pour le premier et 98,5% pour le second. Alors qu'Amazon tire majoritairement ses revenus d'un magasin de vente par correspondance (67,5%), Apple de la vente de l'Iphone (62%) et Microsoft, de ses produits Office et Windows (70,8%). -Voir encadré page 6

Grâce aux cookies, pas les biscuits mais ces petits programmes qui enregistrent les traces de nos passages sur Internet comme le type d'article consulté, la photo qu'on a partagée, les publicitaires peuvent désormais cibler encore plus précisément les consommateurs et espérer les toucher droit au cœur, droit dans leur portefeuille. C'est du sérieux, ce business juteux de près de 80 milliards d'euros rien que pour l'Europe est en constante augmentation.[*]

La collecte des données ne s'arrête pas aux achats en ligne, aux recherches sur Google, aux sites qu'on visite, aux likes, aux livres, émissions, films qu'on identifie sur notre profil Facebook, au streaming, à l'envoi d'e-mails, aux vidéos visionnées sur Youtube, aux commentaires laissés çà et là sur les multiples supports en ligne, aux pétitions signées sur la toile. Nos données sont également recueillies sur les applis qu'on télécharge sur les stores : prévisions météo, calcul d'itinéraire, info trafic, jeux… Mais pas que ! Tous les objets connectés comme le bracelet qui mesure vos pas, les télévisions, les frigos, les robots aspirateurs… et les assistants vocaux (comme Alexa et Google home), censés faciliter votre quotidien, qui enregistrent vos conversations en continu, font partie de cette « famille formidable ».

(*) Le cabinet IDC (conseil et études sur les marchés des technologies de l'information) estime que d'ici 2020, le marché des données des citoyens de l'Union européenne devrait atteindre 80 milliards d'euros.

Mais où est le problème ?

Pourquoi faire une campagne de sensibilisation sur les Big Data ? Au-delà du confort de vie, de la simplification de notre quotidien que peuvent apporter ces nouvelles technologies, elles posent plusieurs questions. Philosophique : vendre notre intimité, notre vie privée à des entreprises privées. Economique : des entreprises se font du fric sur notre dos.

Mais plus largement, c'est tout un modèle de société qui est questionné : sommes-nous d'accord, comme c'est déjà le cas aux Etats-Unis, de permettre à des assurances d'avoir accès à nos habitudes alimentaires, à nos activités sportives pour en contrepartie nous proposer des prix intéressants à condition que l'on ait le bon style de vie ? Serions-nous d'accord avec le fait de permettre au Fisc de contrôler notre train de vie sur base de notre vie virtuelle ? Seriez-vous d'accord de vous faire arrêter sur base d'un « profil à risque de délit » et non pas parce que vous avez réellement commis un délit ? Aujourd'hui, c'est encore de la science-fiction. Mais à Santa Cruz par exemple, la police utilise un algorithme qui « *fournit aux policiers des tendances, des probabilités, des intervalles temporels et des zones géographiques où les crimes ont une forte probabilité d'être commis*[5] ». Un algorithme a également été remis en question par des journalistes d'investigation américains : COMPASS. Celui-ci permet de prédire le degré de récidive d'un individu et est utilisé par les juges aux USA pour les aider dans leurs décisions. L'enquête des journalistes a révélé que les personnes noires étaient pointées comme étant plus susceptibles de récidiver et ce sur aucune base factuelle qui le justifierait[6].

Algorithmes, ces nouveaux juges ?

Comme tout outil statistique, les algorithmes ne sont pas à l'abri d'un biais et ils ne sont pas des entités neutres. La plupart du temps, ce sont des entreprises privées qui investissent dans ces technologies. Cela pose la question des objectifs poursuivis au travers des algorithmes qu'ils financent ou créent directement. Et les pouvoirs publics dans tout ça, censés être les garants de l'intérêt général au-delà de l'intérêt purement économique ? Et si c'était un Etat qui développait un algorithme, quelles garanties aurions-nous quant à leur usage pour nos libertés fondamentales ? Et si nous utilisions ces technologies sous une démocratie et que brusquement nous basculions dans des gouvernements totalitaristes ?

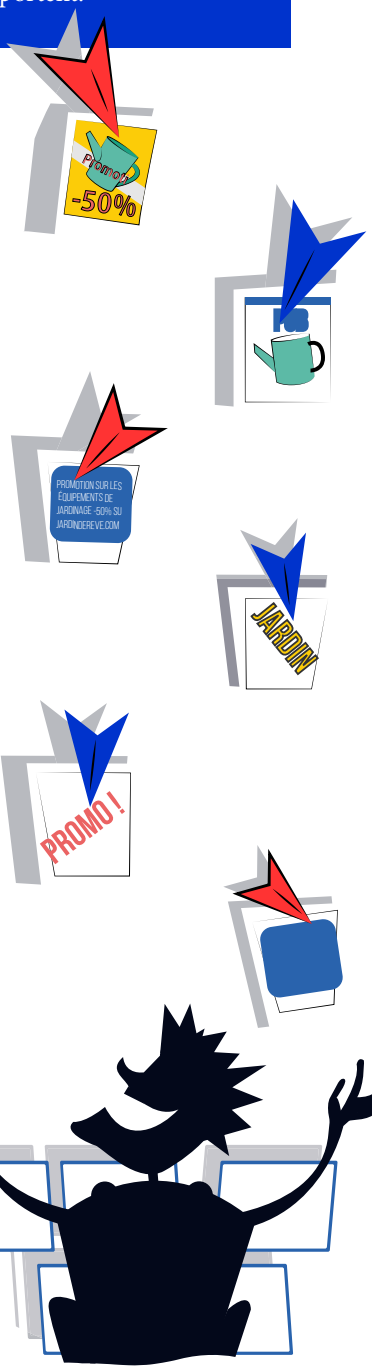
Pas de secrets pour les géants du web

Votre temps, c'est de l'argent pour les GAFA et les annonceurs. Fini les statistiques basées sur des catégorisations classiques. Grâce aux algorithmes, on peut désormais « *saisir le social sur des éléments plus subtils comme le fait que vous vous connectez tard dans la nuit, que vous postez tel type de photo ou de musique, qui permet de déterminer que vous êtes dépressif par exemple […]. Le profil c'est ce qu'on pourrait faire, les personnes avec lesquelles on pourrait avoir des affinités. C'est une projection de nous, une déduction de comportements passés pour déterminer nos comportements futurs* », explique Antoinette Rouvroy (Centre de recherche, info droit et société à l'Université de Namur) au micro de La Première[3]. Et elle ajoute : « *On peut transformer vos likes sur Facebook en des prédictions fiables de vos opinions politiques, religieuses, de votre intelligence, de votre orientation sexuelle ou même si vos parents sont divorcés* ».

Cette « fabuleuse » industrie repose sur les algorithmes, qui sont des énormes ensembles d'opérations ou d'instructions qui permettent de résoudre un problème ou d'obtenir un résultat[4]. Les algorithmes analysent la masse de données générées par nos activités et font un profilage prédictif. Si autant de personnes d'un certain âge, genre, cliquent sur telles et telles informations, et qu'elles partagent telles photos alors elles seraient susceptibles d'être intéressées par tel type de produit (publicité pour un festival rock, pour un site de vente de vêtements…). Ces données sont anonymisées, c'est-à-dire qu'en théorie, on ne pourra plus lier ces données à la personne auxquelles elles se rapportent.

Plus près de nous, la firme britannique Cambridge Analytica qui a travaillé sur la campagne numérique de Donald Trump a défrayé la chronique, accusée d'avoir volé les données personnelles de 87 millions d'utilisateurs de Facebook dans le monde. Et l'a sans doute aidé à remporter les élections de la présidence américaine : « *Donald Trump parlait aux gens avec Twitter, et a gagné avec Facebook* », a résumé Brad Parscale, le responsable de la campagne numérique de Donald Trump dans un entretien accordé à CBS diffusé en octobre 2017[7].

Cet évènement soulève plusieurs questions : nos données personnelles sont-elles suffisamment sécurisées ? Pouvons-nous remettre notre confiance dans des entreprises privées ? Facebook était au courant des faits depuis 2015 et n'en a pas touché un mot avant de les confirmer une fois ces derniers médiatisés par un lanceur d'alerte. De plus, cet épisode prouve que les données personnelles souvent considérées comme anodines, recèlent une puissance considérable au point d'influencer notamment le résultat d'une élection.



Revenons à la toile, le cyber-espace, cette conjoncture de signaux, autant de moyens d'expressions, de fragments de vie, d'empreintes échangées, laissées par des humains du monde entier, autant de traces que l'on a trouvé le moyen de monnayer dans notre société post-industrielle : « *Depuis dix ans, on revient à l'assujettissement des corps sous une autre forme que dans les années soixante via le*

travail à la chaîne, maintenant on consomme et on produit en ligne. En acceptant que l'humain devienne une information qu'on va pouvoir traquer, marchandiser, on accepte le renoncement d'une part d'humanité au nom de la croissance, ce qui fut le cas avec la société industrielle. Finalement, les temps n'ont pas tant changé que ça »[8], explique l'économiste Daniel Cohen.

La technique comme religion ?

Nous sommes dans une société qui vend la promesse qu'on ne manquera de rien, que tous nos désirs seront assouvis, facilités par les technologies. On est, comme le dit Antoinette Rouvroy[9], dans « *un capitalisme de réputation, dans une société de l'évaluation : si on n'est pas sur les réseaux sociaux, on n'existe pas. Avant, notre identité était claire : elle nous était transmise, nous n'avions pas besoin de la construire, aujourd'hui, elle ne nous est plus assignée. Elle est une sorte d'idéal à atteindre* ». Notre société est-elle dès lors vouée à continuer à se déshumaniser ? Un faisceau lumineux, comme un espoir de sortir de la désillusion identifiée par l'économiste français Daniel Cohen[10] peut nous guider pour construire cette société que nous désirons tous : « *ne pas accepter que la précarité soit une forme d'existence, ne pas accepter les travers de l'ubérisation, réinventer mai 1968, se saisir de l'intelligence artificielle pour ne pas la subir* ».

Claudia Benedetto

1. D'après Internet World Stats, le monde comptait 4,05 milliards d'internautes en 2017.
2. "Comment Facebook change vos données personnelles en or", *La Libre en ligne*, le 20 mars 2018.
3. Arnaud Ruyssen : *Google, Facebook… Glisse-t-on vers une algorithmocratie* ? Emission La démocratie en question, La première, 11 août 2018.
4. Définition algorithme sur wikipédia.
5. Aux Etats-Unis, la police prévoit les crimes par ordinateur, Martin Untersinger, publié le 13 novembre 2011, www.nouvelobs.com.
6. Etats-Unis : un algorithme qui prédit les récidives lèse les noirs, Andréa Fradin, le Nouvelobs en ligne, le 24 mai 2016.
7. Cité dans l'article : *Quelle a été l'importance réelle de Cambridge Analytica dans la campagne de Trump ?* William Audureau et Martin Untersinger, Le Monde, 21 mars 2018.
8. Daniel Cohen, économiste, Directeur du département d'économie de l'Ecole Normale supérieure, Emission Les temps changent, ça va mal tourner ? France culture, 3 septembre 2018.
9. Arnaud Ruyssen : *Google, Facebook… Glisse-t-on vers une algorithmocratie ?* Emission La démocratie en question, La première, 11 août 2018.
10. Economiste français, directeur du département d'économie de l'Ecole Normale supérieure.

Services : Moteur de recherche.
Modèle économique : basé majoritairement sur la publicité.
Produits phares : YouTube, le système d'exploitation pour téléphones mobiles Android, Google Earth, Google Maps, Google Play.
Chiffre d'affaires 2017 : 110,9 milliards de dollars.

Services : Conçoit des ordinateurs, smartphone… et des logiciels informatiques.
Modèle économique : basé majoritairement sur la vente de ses produits.
Produits phares : Iphone, Ipod, Ipad Macintosh.
Chiffre d'affaires 2017 : 229,2 milliards de dollars.

Services : réseau social qui rassemble les fonctionnalités d'autres entreprises : moteur de recherche, achat en ligne…
Modèle économique : basé majoritairement sur la publicité.
Produits phares : Messenger, What'app, Instagram.
Chiffre d'affaires 2017 : 40,7 milliards de dollars

Services : Plateforme de vente en ligne.
Modèle économique : basé majoritairement sur la vente de ses produits.
Produits phares : amazone.com
Chiffre d'affaires 2017 : 177,9 milliards de dollars.

Services : Vend et développe des systèmes d'exploitation et des logiciels informatiques.
Modèle économique : basé majoritairement sur la vente de ses produits.
Produits phares : Windows, Suite Office (word…)
Chiffre d'affaires 2017 : 90 milliards de dollars.

Source : Statista Digital Economy Compass 2018

GÉOLOCALISATION : LA BANALISATION DE LA SURVEILLANCE

Notre vie numérique est parsemée d'actions, de traces invisibles à l'œil nu que nous laissons derrière nous lors de notre passage sur le net. Ces empreintes sont enregistrées, collectées sur des serveurs par des firmes dans une visée de marketing. Parmi les données, on trouve celle de la géolocalisation. Où que l'on se trouve sur le globe, on peut aujourd'hui identifier notre position. Serions-nous traqués ?

Wifi, balises, relais téléphoniques, Bluetooth, carte SIM :

Souriez, vous êtes tracés !

Vous vous rendez régulièrement cheWz votre petit ami ? Vous êtes tracés. Vous allez souvent à la messe ? Encore tracés. Vous fréquentez les bars gays ? Toujours tracés. Vous passez régulièrement devant tel type de magasin de fringues ? Encore et toujours tracés. Vous allez me dire qu'il suffit de désactiver le GPS de votre téléphone pour être tranquille… sauf que non ! Même si vous désactivez cette option, vous êtes toujours localisable. Comment est-ce possible ?

Il existe plusieurs façons d'identifier votre position :

- Par **GPS**, c'est-à-dire via les satellites.
- Par le **wifi**.
- Par les **relais téléphoniques ou Données mobiles** (2G, 3G, 4G et bientôt 5G !).
- Via le **Bluetooth** et l'installation d'une application sur votre smartphone. En Belgique, la banque KBC utilise ce système via son application mobile.
- Mais aussi via les ***beacons***, balises disposées notamment dans les commerces aux Etats-Unis mais aussi en France et bientôt chez nous. Ce n'est pas de la géolocalisation proprement dite dans le sens où c'est plutôt un système qui vous envoie des messages lorsque vous vous trouvez à proximité. Si on ferme la géolocalisation, les beacons ne sont pas pour autant désactivés.
- La **Carte SIM** de votre téléphone mobile peut également enregistrer des données de localisation. Proximus propose à des sociétés diverses, des données de localisation que l'entreprise collecte sur les cartes SIM des appareils mobiles de ses clients. Ces données sont anonymisées.

Elliot Alderson, vous connaissez ? C'est ce jeune ingénieur en sécurité informatique qui est au centre de la série américaine Mr Robot, que je vous recommande au passage. Ce cyber-justicier anti-système souffrant de troubles de l'anxiété et de paranoïa recouvre sa webcam d'un scotch, se balade dans la rue avec un capuchon sur la tête pour ne pas être identifié par les caméras de surveillance, surfe sur le darknet et utilise tous les subterfuges pour être invisible... Et dans la vraie vie, ça marche comment ?

Toute une série d'applications ont basé leur modèle économique sur la géolocalisation. Par exemple **Tinder**, une appli qui permet d'identifier des personnes célibataires dans les environs d'où vous vous trouvez, mais aussi **Uber** ou **Google Map**. Sans géolocalisation, pas de business pour ces applis. Les systèmes d'exploitation comme Android, qui appartient à Google (l'un des leaders en matière de commercialisation des données personnelles), collectent également des données de géolocalisation.

Les panneaux publicitaires vous épient

Aujourd'hui, il est possible pour les annonceurs d'adapter la publicité qui s'affiche sur votre téléphone mobile **lorsque vous passez devant un panneau publicitaire** ; il suffit pour cela que vous ayez accepté le message de localisation. C'est bien connu, beaucoup de gens qui se baladent en rue aujourd'hui, ont souvent les yeux rivés sur leur smartphone et ne sont pas attentifs à leur environnement. En 2019, on estime que près d'une publicité sur deux envoyée sur nos mobiles sera géolocalisée.(1)

1. Géolocalisation : tous traqués ? Sophie Roland, Vincent Kelner et Dominique Morteau, Envoyé spécial, 12 février 2015.

Une intrusion permanente

Après tout, la plupart des gens aujourd'hui, en partageant un selfie par exemple, indiquent l'endroit où il a été pris, dans quel restaurant ils sont en train de manger ou de boire un verre… Beaucoup partagent leurs bons plans, les hôtels qu'ils fréquentent… Dans ce cas, vous choisissez vous-même d'être localisables, c'est votre propre choix. Mais lorsqu'on vous l'impose, c'est une autre histoire. Et vous n'imaginez pas tout ce que Google récolte sur vous sans votre autorisation, ou en tout cas sans que vous ne le sachiez parce que vous n'avez pas lu les conditions générales. Les firmes qui collectent vos données savent à quelle heure vous allez dormir grâce à l'heure à laquelle vous n'êtes plus actif sur les réseaux sociaux ou sur internet… Elles connaissent vos habitudes : à quelle heure vous sortez de chez vous le matin, si vous déposez vos enfants dans telle école, si vous vous rendez régulièrement dans tel hôtel, où vous allez faire vos courses…

Du coup, même si vous essayez de soigner votre identité numérique, que vous contrôlez les photos de vous que vous postez, que vous ne mentionnez pas les restos où vous vous rendez, les algorithmes des grandes sociétés qui récoltent les données, eux, seront capables de mettre à jour votre vraie identité, votre identité physique, celle que vous voulez cacher derrière vos selfies sur les réseaux sociaux.

De plus, les **objets connectés** qui commencent à faire partie de notre quotidien présentent d'énormes failles. Par exemple, les montres qui enregistrent notre rythme cardiaque et nos trajets, ou les poupées connectées censées apporter une sécurité à vos enfants, sont facilement « piratables ». Il en existe tout de même qui sont plus sécurisés que d'autres ; renseignez-vous bien lors de l'achat de l'un de ces nouveaux joujoux !

Les données de géolocalisation sont encore plus intrusives que les autres types de données que l'on collecte sur nous.
En 2014, la CNIL (Commission nationale informatique et libertés)[1] a publié une étude réalisée pendant trois mois sur les deux cents applications les plus utilisées par les Français. Celle-ci a révélé que 30% des applis ont eu accès à la localisation. **L'appli météo** ou **l'appli Playstore** installées par défaut sous Android, ont chacune géolocalisé les smartphones en test 1,5 million de fois pendant 3 mois à savoir 10 accès par minute ! Par contre, sur IOS, le système d'exploitation mobile développé par **Apple,** moins de données sont mesurées que sous Android, système d'exploitation mobile développé par Google.

A quelles informations ces applications ont-elles accès ? Au nom de l'opérateur, au numéro de série du téléphone, au numéro de téléphone, aux identifiants de la carte SIM, à la liste des points d'accès wifi : ceux-ci sont cartographiés dans le monde. En ayant accès à la liste des wifi déjà utilisés par votre téléphone, on va pouvoir déterminer les lieux où vous vous êtes rendus.

Le géomarketing a de beaux jours devant lui. Il permet d'ajuster un message en fonction d'un territoire donné. Par exemple, en analysant les données du site internet qu'une société gère, elle peut se rendre compte qu'elle a moins de visites de personnes qui se trouvent dans la province du Luxembourg. Elle peut alors prévoir une campagne de communication pour attirer ces personnes-là, par exemple, en leur proposant une offre d'abonnement alléchante. Vous l'aurez compris, si vous vous trouvez à Bruxelles, vous n'aurez pas le même avantage.
Vous avez sans doute aussi remarqué que depuis quelque temps, les sites ou **applis de médias en ligne** vous proposent de vous localiser. Cela leur permet de vendre cette donnée à des publicitaires qui pourront ainsi adapter l'offre à votre localité.

Du marketing au flicage

Qu'un inconnu connaisse vos trajets quotidiens ou vos comportements d'achats n'a peut-être pas beaucoup d'importance pour vous. Mais c'est sans compter sur l'énorme pouvoir qu'ont les sociétés qui détiennent toutes ces données sur nous : que diriez-vous de devoir utiliser une appli qui enregistre votre comportement de conduite en temps réel ? En échange, votre assureur vous donnerait une ristourne si vous obtenez un bon score ! Certaines entreprises utilisent également cette technologie pour surveiller leurs salariés : suivre leur temps de travail, les livraisons… Bien qu'un cadre juridique existe, c'est la question de la banalisation de la surveillance qui est en jeu.
Entre sécurité et surveillance, la distance est ténue. Au nom de la sécurité, on justifie l'usage de technologies qui nous épient. La surveillance est brandie comme un moindre mal, une évolution naturelle et l'on doit faire confiance aux autorités qui ont accès à notre vie privée. Comment faire aujourd'hui si l'on ne souhaite pas être tracé ? Etre attentif au type d'applis que l'on télécharge ? Désactiver le GPS de son téléphone et de son appareil photo ? Couper le wifi, les données mobiles et le Bluetooth ? Est-ce pour autant envisageable ? En théorie sans doute. Qui va penser à chaque fois qu'il aura terminé d'utiliser son smartphone, à réaliser ces actions ?

Au-delà de la prise de conscience des individus, de la nécessaire information, de l'échange utile de trucs et astuces, c'est le modèle

1. La Commission nationale de l'informatique et des libertés (CNIL) est une autorité administrative indépendante française. La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'Homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

qu'il faut questionner : est-ce normal que Google Maps soit l'application de référence utilisée par d'autres applis ? N'y a-t-il pas là un problème de monopole et donc de concentration de données dans les mains de quelques géants du Net ? Des alternatives existent mais elles ne sont pas suffisamment connues (Startpage, Openstreetmap…) et manquent de moyens pour se perfectionner et proposer des outils aussi faciles à utiliser que l'offre Google. Une solution serait de demander aux autorités compétentes de promouvoir et investir dans ce type de projet.

Est-ce normal que certains pays européens utilisent les données, notamment de géolocalisation, des migrants pour vérifier leurs dires ? N'est-ce pas là une grave atteinte aux droits de l'homme ? N'est-ce pas là aussi le signal d'une dérive ? Qu'est-ce qui nous garantit que nos faits et gestes resteront consignés à un seul endroit ou seront utilisés uniquement à des fins clairement identifiées ? Et plus simplement, avons-nous, sans nous en rendre compte, abandonné à jamais notre droit à l'anonymat, le plaisir de nous fondre dans la masse, de nous perdre au détour d'une ruelle sans pour autant que des inconnus parfois même à l'autre bout du monde ne soient au courant ? Avons-nous délaissé une fois pour toute la sensation enivrante que peut procurer la liberté de mouvement ?

Claudia Benedetto

Trahis par le Bluetooth…

Certains centres commerciaux en France et maintenant en Belgique vous proposent une appli qui vous renseigne sur les promotions et qui vous guide vers le produit que vous désirez. Attendez-vous à recevoir une flopée de notifications au moindre mouvement, dès que vous passez devant les magasins mais aussi dans leurs enceintes. Vous n'êtes que de passage dans le rayon des sous-vêtements, qu'importe ! Votre téléphone sonne pour vous rappeler qu'il y a une promo à saisir sans tarder. Vous ne comptiez pas acheter de brosse à dents aujourd'hui ? Pas grave, votre smartphone est toujours là pour vous rappeler qu'une offre incroyable est à portée de main ! Comment cela est-il possible ? Il suffit de vous géolocaliser sur l'appli du centre commercial, d'activer votre Bluetooth et le tour est joué : une petite boite noire installée dans les magasins vous renvoie un signal quand vous passez à proximité. C'est une aubaine pour les commerçants qui leur permet d'analyser vos goûts, identifier le rayon le moins attractif et trouver une stratégie pour vous y attirer quand même. En Belgique, cette technologie n'est pas encore bien implantée, mais à Namur et à Bruxelles, des balises ont été installées sur les devantures de certains magasins : l'application qui permet de faire fonctionner le dispositif a déjà été téléchargée par plus de 1.000 personnes.

Trois lieux suffisent pour connaître vos amis !

Vous localiser permet d'avoir accès à toute une série d'informations vous concernant : « *Pour identifier de manière unique une personne, il suffit d'avoir accès à trois points de géolocalisation. Parce que personne n'a le même triplé d'informations : personne n'a le même travail que vous ; le même domicile que vous, le même loisir que vous* » explique Stéphane Petitcolas, ingénieur expert à la CNIL, à l'occasion des Assises du Géomarketing 2015 [1].

Tout cela est possible par exemple en analysant la fréquence à laquelle on vous localise à un endroit précis. Mais ce n'est pas tout ! On peut aussi savoir qui sont vos vrais amis dans la vraie vie ! Pour ce faire, les analystes qui réceptionneront vos données analyseront le nombre de fois que vous vous trouvez au même endroit qu'un autre appareil, si cela se reproduit quatre fois, on pourra en déduire que vous êtes avec un proche.

1. Stéphane Petitcolas présente la protection des données personnelles sur l'utilisation de la géolocalisation par les smartphones à l'occasion des Assises du Géomarketing 2015.

Le nouveau RGPD

UN PARAPLUIE POUR PROTÉGER SES DONNÉES PERSONNELLES

Nous avons tous entendu parler du fameux RGPD, le nouveau règlement européen sur la protection des données personnelles, entré en vigueur en Europe depuis le 25 mai dernier. De qui s'agit-il ? Nous protège-t-il de tous les abus en matière d'utilisation de nos données personnelles à des fins commerciales ?

En Europe, nous sommes mieux protégés que dans d'autres pays (comme les Etats-Unis par exemple) face à la numérisation croissante et assauts du marché publicitaire. Le RGPD a encore renforcé cette protection, avec cependant quelques bémols.

Le RGPD[1] (*Règlement général sur la protection des données*) est entré en vigueur le 25 mai 2018. Il prévoit de nouveaux droits et obligations en termes de protection des données personnelles. L'intention du RGPD est qu'il y ait plus de transparence vis-à-vis des consommateurs, afin qu'ils sachent ce qu'il advient de leurs données personnelles, à qui leurs données sont transférées, dans quel but elles sont traitées...

Que recouvre la notion de données personnelles ?

Ce sont toutes les informations qui permettent d'identifier une personne de façon directe ou indirecte, comme par exemple : un nom, une adresse, une photo, un identifiant, un numéro de téléphone, une plaque d'immatriculation, une carte de crédit, un dossier médical… La définition du RGPD inclut également les données de géolocalisation ou encore le profilage.

Et le responsable de traitement, c'est qui ?

C'est l'entreprise, l'autorité publique, l'organisme qui décide « pourquoi » (l'objectif de la récolte de données) et « comment » (par quels moyens) vos données personnelles devront être traitées. Le RGPD s'impose à toute entreprise, européenne ou internationale, qui propose des biens ou services sur le marché européen. Dès qu'une entreprise collecte des données à caractère personnel sur un citoyen européen, alors le RGPD s'applique.

Les grandes nouveautés introduites par le RGPD

MINIMALISATION. Seules les données pertinentes et limitées à ce qui est nécessaire par rapport à l'objectif poursuivi peuvent être récoltées. Si davantage de données personnelles sont demandées au consommateur par rapport à ce qui est nécessaire, cela entre en conflit avec le RGPD. C'est le principe de limitation, de minimalisation des données.

Un exemple. Votre nouvelle banque propose des prêts au logement à des taux intéressants. Vous achetez une nouvelle maison et décidez de changer de banque. Vous demandez à votre ancienne banque de clôturer tous vos comptes et de supprimer toutes vos données à caractère personnel. L'ancienne banque est toutefois soumise à une loi qui l'oblige à conserver toutes les informations relatives à ses clients. L'ancienne banque ne peut donc pas supprimer vos données, mais vous pouvez lui demander de ne conserver les données que durant la période exigée par la loi et ne plus s'en servir à des fins de marketing.

INFORMATION, OPPOSITION, EFFACEMENT. De plus, les droits existants comme le droit d'être informé sur la finalité du traitement, le droit d'opposition et à l'effacement des données sont mieux contrôlés et encadrés.

PORTABILITE. Autre nouveauté : le droit à la portabilité des données. A l'avenir, le consommateur pourra demander à un prestataire de service de lui fournir ses données personnelles dans un format courant et lisible facilement, et de les transmettre à un autre prestataire de service.

Problème : Le droit à la portabilité ne vise que les données personnelles que le consommateur a « activement » fourni au responsable de traitement (photos, commentaires…). Mais quel sort est réservé aux autres données « générées » par le consommateur (comme les données de localisation ou les cookies par exemple) ? Sont-elles aussi visées par ce droit à la portabilité ? Le RGPD est malheureusement muet sur ce point. Par ailleurs, le RGPD ne dit rien non plus quant à une éventuelle utilisation ultérieure des données transférées par le premier opérateur. Sera-t-il autorisé à le faire ? Devra-t-il informer le consommateur ?

CONSENTEMENT. Le consentement doit être demandé de manière **claire et concise**, en utilisant des termes faciles à comprendre, et se distinguer clairement des autres informations telles que les conditions de vente. La demande doit préciser l'usage qui sera fait de vos données à caractère personnel et comprendre les coordonnées du responsable qui traite les données. Et le consentement doit être donné de manière volontaire.
Un exemple. Le consentement peut être donné en cochant une case sur un site internet ; il ne sera par contre pas valable si la case est pré-cochée à l'avance. *Et le consommateur pourra retirer son consentement à tout moment et tout aussi facilement qu'il l'a donné. Par exemple, en cliquant sur un lien de désinscription en bas d'une newsletter qui vous est envoyé.*

Quels recours pour le consommateur ?

Vous devez tout d'abord contacter le responsable du traitement. Celui-ci doit répondre à votre demande dans les meilleurs délais et au plus tard dans un délai d'un mois. Si vous estimez son motif injustifié ou s'il ne vous répond pas du tout, vous pourrez déposer une plainte à l'Autorité de protection des données[2].
Trois options possibles :

- Déposer une réclamation auprès de l'Autorité de protection des données[3]

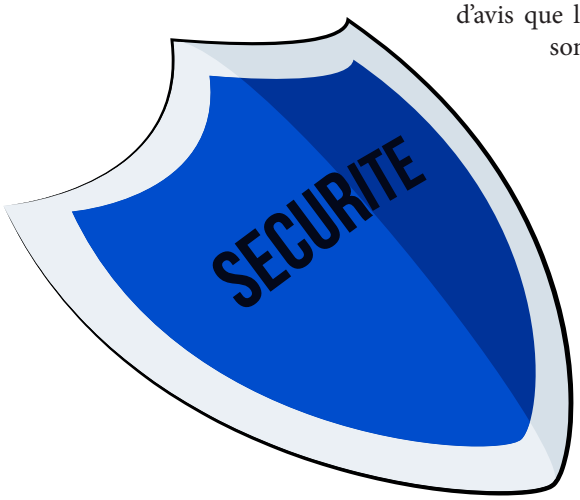
Ses missions sont notamment de recevoir les plaintes des citoyens, de sensibiliser le public sur la protection des données personnelles, de surveiller la bonne application du RGPD et d'imposer des amendes.

- Intenter vous-même une action en justice

Désormais, vous pouvez demander au responsable du traitement concerné une réparation du dommage subi (cela peut être une perte financière ou une perte de réputation), en allant devant un juge.

- Intenter une action collective

Si vous ne voulez pas déposer une réclamation individuelle auprès du tribunal, vous pouvez mandater une organisation (telle que Test-Achats) qui pourra agir en votre nom.
Ce type d'action collective devrait augmenter considérablement car, finalement, les violations du RGPD affecteront un grand nombre de personnes. Pensez par exemple à une "fuite de données". À l'avenir, un recours collectif dans ce contexte est donc possible. Non seulement l'action collective pourra contribuer à augmenter l'effectivité des droits des consommateurs, mais une action collective permet aussi de partager les coûts de procédure. Le RGPD permet également aux organisations de faire une réclamation collective indépendamment du mandat des personnes impliquées. Ce sont des cas dans lesquels cette organisation est d'avis que les droits des personnes impliquées ont été violés. La Belgique n'utilise malheureusement pas cette option (pour le moment).



Que dit le RGPD sur le profilage des consommateurs ?

Le profilage automatisé est devenu très courant dans le domaine du marketing. Cette méthode peut limiter vos choix et vous porter préjudice.

Le profilage a lieu lorsque vos aspects personnels sont évalués afin de réaliser des prédictions à votre sujet, un profil de vos goûts et préférences. Par exemple, si une entreprise ou une organisation évalue vos caractéristiques (telles que votre âge, votre sexe, votre taille) ou vous classe dans une catégorie, cela signifie que vous êtes profilé. Le RGPD donne une très large définition du profilage qui inclut notamment la publicité ciblée et la géolocalisation.
Un exemple : vous avez acheté deux tickets pour assister à un concert auprès d'une société de vente de tickets en ligne. Par la suite, vous êtes submergé de publicités pour des concerts et événements qui ne vous intéressent pas. Vous informez la société de vente de tickets en ligne que vous ne souhaitez plus recevoir de publicité. La société doit arrêter de vous en envoyer.
Problème : Encore une fois, ce droit n'est pas absolu car c'est au responsable de traitement à évaluer si la méthode de profilage du consommateur est susceptible de l'affecter. Comment ? Selon quels critères ? Le silence du RGPD risque de causer préjudice au consommateur.

Conclusion : "Bien", mais aurait pu mieux faire

Certes, les objectifs du RGPD sont louables : assurer plus de transparence pour le consommateur, afin qu'il soit mieux informé de ses droits, et qu'il devienne plus « consom'acteur ». Lui octroyer de nouveaux droits, comme le droit à l'accès et à la portabilité de ses données, le droit à la limitation du traitement, sont de très belles avancées dans un monde digital qui ne cesse de prendre de l'ampleur.
Cependant, permettre des limitations à l'exercice de ces nouveaux droits remet en question leur plus-value pour le consommateur. De plus, sur certains aspects, le RGPD est muet, ne précise pas assez les termes employés. La porte est (trop) souvent ouverte au responsable de traitement dans l'évaluation de l' intérêt des parties concernées. Où sont les garde-fous ?
Nous devrons donc rester extrêmement attentifs à la lecture du RGPD qui sera faite par la Cour de Justice de l'Union européenne et à la bonne application de celui-ci en regard des décisions qui seront prises par l'Autorité de protection des données (pourvues qu'elles soient rendues publiques…).

Caroline Sauveur, AB-REOC

Analyse plus complète du RGPD disponible sur http://www.equipespopulaires.be/actualites/

1. Règlement (UE) 2016/679 du Parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/ce.
2. https://www.autoriteprotectiondonnees.be/
3. Idem

COMMENT NOS DONNÉES N

LES COOKIES

Les « cookies » constituent le fonctionnement principal par lequel nous laissons échapper toute une série de données personnelles lors de nos navigations sur Internet.
Un cookie est l'équivalent d'un petit fichier texte, déposé sur la mémoire de nos ordinateurs, qui stocke certaines informations lors de notre visite d'un site. Certaines informations peuvent être très utiles voire indispensables, y compris pour nous. D'autres sont utilisées à des fins publicitaires. Les cookies ne sont pas des virus ni des logiciels espions.

On distingue plusieurs types de cookies :

- Les cookies de session : temporaires, ils sont surtout utilisés par les sites d'achat en ligne pour mémoriser votre panier, vos informations de commande, etc.
- Les cookies permanents servent à retenir les informations nécessaires à notre connexion sur un site, par exemple (identifiant, mot de passe si on le souhaite, numéro de compte, etc.)
- Les cookies internes, générés par le site visité, servent à enregistrer nos préférences, nos comportements d'utilisateur (par exemple, les types de rubrique qu'on consulte le plus souvent sur un site d'info)
- Les cookies tiers, eux, sont créés par un site tiers et actifs sur le site consulté afin d'enregistrer des informations essentiellement à des fins de marketing ciblé.

Même au repos, notre smartphone travaille beaucoup !
Ni vu ni connu, les utilisateurs de smartphone utilisant Androïd permettent à Google de collecter en moyenne 340 données en 24h s'ils laissent le navigateur Google Chrome ouvert, même en arrière-plan ! 35% des données collectées sont des informations de géolocalisation. (Étude menée par Douglas C. Schmidt. LLB du 29/08/18)

LA GEOLOCALISATION

Kézako ? Système qui permet de vous localiser de manière assez précise via le GPS de votre téléphone, le Wifi, les relais téléphoniques (2G, 3G et 4G) et les Beacons (ou boites noires) apposés sur les devantures des magasins.

Type de données collectées ? Votre adresse, l'école fréquentée par vos enfants, les bars et lieux culturels que vous affectionnez, les lieux de culte que vous visitez, le degré de proximité que vous avez avec un contact qui se trouve dans votre répertoire téléphonique, le nombre de fois par semaine que vous faites vos courses, quels sont les commerces que vous fréquentez mais aussi le produit que vous venez de regarder dans un magasin…

Par qui ? Les principaux collecteurs de données sont les GAFAM mais aussi les commerçants, les médias en ligne…

A quelles fins ? Pour adapter l'offre publicitaire à votre territoire et cibler ainsi au mieux le message publicitaire à votre profil.

Quelles applications utilisent la géolocalisation ? Google Maps, Waze...

« À
l'algo
autant
A partir
connait
famille.
likes, il
que vot
Thom

IOUS ÉCHAPPENT-ELLES ?

LES RÉSEAUX SOCIAUX

Facebook, Instagram, Twitter, Snapchat, Google+, Pinterest… autant de réseaux sociaux qui collectent et vendent quotidiennement des milliards de données. Autour d'eux gravitent des « satellites » tels que Whatsapp, Messenger, Spotify, Youtube, Shazam, etc., qu'ils ont acquis pour augmenter leurs positions sur le marché des données.
Quels types de données confions-nous aux réseaux sociaux en acceptant les conditions générales d'utilisation (CGU) lors de notre inscription ?

- D'abord les informations générales de profil : nom, prénom, âge, sexe, liste d'amis, emplois, études, lieu de vie, famille, etc.
- Mais aussi et surtout, tous nos likes, commentaires et partages, participations à des événements, et même la simple consultation d'autres pages ou publications : toutes ces activités additionnées permettent de nous donner un profil très précis (même si on ne s'en rend pas compte)
- Notre historique de localisation, les temps de connexion, la fréquence de consultation, etc. contribuent à affiner encore ce profilage.

Ces données circulent : elles sont vendues à des annonceurs publicitaires. Et ces données s'entrecroisent : on peut s'inscrire sur un site d'info ou sur une messagerie via notre profil Facebook par exemple.

Bon à savoir : Facebook sait presque tout de vous, mais il collecte aussi les coordonnées de vos amis, y compris leur numéro de téléphone. Soyez donc vigilants dans votre intérêt mais aussi dans le leur !
Comment accéder à vos informations et paramétrer votre compte ? Voir page 18.

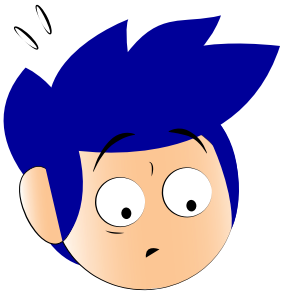
LES APPLICATIONS

Avec les cookies, les réseaux sociaux et la géolocalisation, les applications sont une source inépuisable de données personnelles pour les GAFA.

Il en existe des milliers à notre disposition sur notre smartphone, lorsque vous ouvrez votre *Play store*, *Apple store* ou *Microsoft store*. Vous y trouverez en particulier des jeux et du divertissement pour petits et grands. Mais aussi des applications « utilitaires » come la météo, l'enregistreur vocal, la traduction, la lampe de poche, la calculatrice, le régime alimentaire…
Ou encore les applications bancaires, celles des agences de voyages et des sites de réservation en ligne (booking.com) pour vous faciliter l'accès à leurs services.
Certaines sont payantes, la plupart sont gratuites… car la collecte des données que vous leur laissez en les utilisant sont très rentables pour elles !

Interview

"DES ENJEUX ÉCONOMIQUES ET DÉMOCRATIQUES"



Pour THOMAS LEMAIGRE [1], ce n'est vraiment pas une bonne idée pour la démocratie qu'on soit tous espionnables à merci. Et le formatage des offres de contenus qui s'opère grâce aux algorithmes réduit à notre insu nos goûts et notre horizon de pensée. Il ne prône pas l'abstinence numérique, mais le développement de l'esprit critique et la création d'outils numériques pour préparer la contre-attaque.

La puissance des Big Data s'est construite sur l'immense masse de données récoltées. Par quel biais ces informations sont-elles captées ?

Il n'y a pas qu'un seul fonctionnement, et c'est cela qui fait la force des Big Data. Elles se constituent par des canaux différents et complémentaires. L'histoire d'Internet se double d'une histoire de la récolte de données, qui devient de plus en plus élaborée. Prenons l'exemple des **cookies**. Il s'agit à l'origine d'un petit fichier texte stocké dans votre disque dur, qui est un aide-mémoire pour votre navigation sur Internet. Le cookie enregistre localement des données de connexion pour qu'à votre prochain passage sur le même site, une série d'informations soient préenregistrées.

C'est un premier moyen, basique, de collecte de données. Mais cette technologie est tellement simple qu'elle a donné lieu à des tas de développements. Et cette récolte de données se déroule à faible bruit, c'est-à-dire sournoisement. Même si on a vu passer le message, à présent obligatoire, qui nous demande d'accepter l'utilisation de ces cookies, savons-nous réellement ce que cela implique ? La collecte de données est énorme. Une partie de la collecte de Big Data s'opère grâce aux réseaux sociaux, comme **Facebook**, qui est capable de collecter énormément d'informations uniquement à partir de ses propres fonctionnalités, à partir des comportements des utilisateurs : les likes, les partages, etc. Il ne se limite pas à cela, bien sûr, car il y a souvent un échange de données avec des sites tiers.
Par exemple, on a la possibilité de se connecter à des sites internet ou des plateformes par l'interface de notre compte Facebook ou Google+. Ce faisant, il y a un échange de données. Si l'on se connecte de cette façon sur RTBF-Auvio par exemple, Facebook est en capacité de récupérer des données liées à notre utilisation d'Auvio.

Ce qui a donné le coup d'accélérateur aux Big Data, c'est l'apparition du smartphone. Les applications qu'on utilise abondamment fonctionnent comme des petits mouchards sur toute une série de comportements. La géolocalisation évidemment est l'une des sources d'information possibles. Mais le simple fait de laisser son smartphone Android allumé avec la navigateur Chrome ouvert en tâche de fond permet à Google de collecter des données vous concernant en moyenne toutes les 4 minutes 25 secondes ! Et tout ceci n'est encore rien à côté de ce que vont permettre à leurs opérateurs les objets connectés, la reconnaissance vocale ou la voiture sans pilote...

Les enjeux ne sont donc pas seulement commerciaux. Il faut prendre conscience des potentialités antidémocratiques du Big Data. On a maintenant des applications qui permettent de faire des paiements directs au moyen de QR codes, sans passer par une carte ou de la monnaie. Un tel dispositif enregistre un tas d'informations sur nos achats, en l'occurrence. En Chine, on en est déjà à du ranking social, avec

1. Thomas Lemaigre, chercheur indépendant, enseignant, co-directeur de la Revue Nouvelle

des algorithmes qui calculent votre niveau de civilité à partir de données récoltées sur les comportements. Est-ce que vous avez rendu votre voiture de location en retard ? Est-ce que vous êtes arrivé en retard à l'école de vos enfants ? Etc. Cela peut aller très loin.

Rassurez-nous, en Europe nous n'en sommes pas encore là…

Je ne sais pas précisément où on en est. Mais en Europe, on a heureusement une législation sur la protection de la vie privée et des données personnelles qui est quand même plus ou moins respectée par les firmes de droit européen. ING ou Belfius, par exemple, ne peuvent pas faire des choses aussi délirantes que cet exemple chinois, mais BNP Fortis et KBC proposent Google Pay depuis quelques mois, sans avoir les moyens de vérifier que leur sous-traitant Google respecte complètement le RGPD. Mais cela signifie aussi, et c'est une critique que certains chantres du numérique ne se privent pas de faire, que l'Europe renonce à une partie de sa compétitivité dans cette économie des données. Ce qui laisse le champ à d'autres acteurs de droit américain ou chinois… J'ai récemment lu une carte blanche qui alertait sur le retard européen en matière de synthèse vocale, à cause entre autres de nos législations plus contraignantes en matière de vie privée. Cet argument existe.

Est-ce que c'est Big Brother ? Doit-on vraiment avoir peur pour la protection de notre vie privée ?

Je pense qu'il est justifié d'avoir peur, mais pas seulement pour cette raison-là. Je pointerais deux aspects. Il y a d'abord, effectivement, le fait que ce n'est pas une bonne idée, pour la démocratie et la cohésion sociale, qu'on soit tous espionnables à merci par des organismes qui n'ont de comptes à rendre qu'à eux-mêmes. Quand on va voter, il y a un rideau à l'isoloir, et ce n'est pas pour rien. Cela permet de nous soustraire à toute une série de pressions potentielles, de rapports sociaux, de dominations même symboliques. La possibilité de vivre en-dehors du regard d'autrui est quelque chose de fondateur pour les démocraties modernes. Ce n'est pas une question de pudeur ou d'intimité, cela engage la société dans son ensemble.

Et l'autre raison d'avoir peur, qu'Yves Citton ou Antoinette Rouvroy montrent très bien, c'est que les algorithmes formatent nos vies. Ils anticipent nos jugements, prédéfinissent nos comportements, conditionnent notre expérience, notre rapport à la culture, à la vie politique, etc. Cela nous détourne de notre propre autonomie en tant qu'individus, de notre libre-arbitre. Ce qui est vicieux, c'est que cela se joue à l'insu de notre conscience. Et ce faisant, à travers les Big Data, nous laissons des entreprises réduire notre champ d'expériences, de découvertes, de surprises, de curiosités. Dans le domaine de la consommation culturelle, c'est assez flagrant. L'algorithme d'Amazon nous prescrit des livres sur base de ce que nous avons déjà lu, de ce que nos amis ont acheté, voire des articles qu'on a lus sur tel site d'info, et c'est très séduisant évidemment. Mais c'est un formatage de notre accès à une masse culturelle pourtant infinie. (Cf. l'article en page 17)

Le problème que posent les Big Data se situerait donc davantage en matière de formatage culturel de la consommation qu'en termes de risque pour la démocratie ?

Il y a quand même eu l'affaire Snowden, qui révèle que les grands oligopoles de l'économie des données ne sont pas des pères-la-vertu. Ces oligopoles ont donné accès aux services

C'est quoi, au fond, le Big Data ?

Je pense qu'il ne faut pas confondre le fait que les technologies de l'information permettent de traiter énormément de données, et les Big Data au sens où on l'entend généralement. La banque-carrefour de la Sécurité sociale par exemple, qui est une base de données publique, ce n'est **pas** du Big Data. Ce sont des systèmes fermés, sécurisés, contrôlés, organisés, normés par des législations. N'importe qui n'y a pas accès, on ne peut pas les utiliser pour n'importe quoi. Ce n'est pas parce que les bases de données sont gigantesques que c'est du Big Data. Les données d'une administration publique sont complètes, hyper structurées, et ce de façon homogène pour des millions de personnes, structurées en fonction des mêmes champs.

Le Big Data, c'est l'inverse. C'est ce que les statisticiens appellent de la donnée sale. C'est bordélique, ça part dans tous les sens. Ce sont des données qui viennent de sources diverses, non coordonnées, qui ne sont donc pas structurées de la même façon. Mais elles existent en une telle quantité qu'il y a, malgré tout, moyen d'en tirer quelque chose à l'aide d'algorithmes de plus en plus performants. Ils tirent, d'une immense masse de données plutôt mal foutues, des informations dont il est possible de se servir. Ces données sont la propriété des entreprises qui les captent. C'est tout le sens des conditions générales d'utilisation (CGU). Vous ne les lisez pas, évidemment ! Mais vous cochez la petite case, et avalisez du coup le fait que vous acceptez que vos données soient utilisées, qu'elles deviennent la propriété du site ou de la plateforme sur lesquels vous créez un compte. Ces données ont bien sûr une valeur économique. Il y a un marché de ces données, très florissant, avec des courtiers. Cela permet de se constituer de gigantesques bases de données, comme quand MasterCard vend des informations à Google, avec des parties plus ou moins propres, d'autres très chaotiques.

secrets américains et anglais à des quantités infinies de données, à leurs systèmes de calculs, à leurs algorithmes, etc. Le programme américain PRISM défie l'imagination. En tant que militant associatif ou politique, a-t-on envie que ce qu'on pense, ce qu'on imagine comme projet ou comme action collective se retrouve sur la place publique, traité par des services de renseignement ? C'est quelque chose dont on a longtemps imaginé qu'il serait impossible en Europe. Dans le domaine de l'aide sociale par exemple, les assistants sociaux dans les CPAS ont la possibilité de scruter les comptes Facebook de gens qui demandent le RIS. Le fisc aussi, ou bien sûr les employeurs qui recrutent. Il y a donc des limites qui sont en train d'être franchies, qui interrogent notre conception de la démocratie.

Comment réagir à cette situation ? Faut-il se déconnecter totalement ? Ou agir collectivement ? Que recommanderiez-vous comme attitude ?

Je ne crois pas qu'il faille dire aux gens ce qu'ils doivent faire. Les gens en ont marre, de toute façon, qu'on leur dise quoi faire. Ce qui me semble important par contre, c'est de faire de la pédagogie, de montrer les conséquences de notre participation à cette économie du Big Data. Nous sommes des millions à être poussés à adopter les mêmes comportements : il me semble donc nécessaire de chercher des explications systémiques, globales pour comprendre comment ces comportements sont éventuellement suscités par des acteurs économiques qui ne sont pas neutres. Il s'agit de prendre conscience des conséquences au niveau individuel et au niveau collectif. Faut-il conseiller de crypter ses mails, fermer son compte Facebook, désactiver la géolocalisation sur son smartphone ? Sincèrement, je ne sais pas. Mais par contre, je trouve qu'il est vraiment essentiel d'avoir une éducation numérique minimale pour que chacun ait des outils pour saisir cette économie des données et de l'attention dans laquelle il joue, quelles sont les règles du jeu si on gratte un peu sous la surface. C'est un peu l'idée de votre campagne, non ?

Réduire la quantité de données qu'on cède, augmenter le niveau de vigilance, ce n'est de toute façon pas une mauvaise chose…

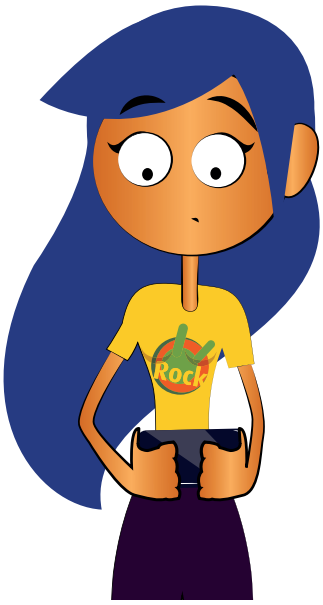
Bien sûr. Le questionnement à avoir, c'est : est-ce que notre projet de vie est de devenir des sortes de vaches à lait de multinationales peu scrupuleuses et surtout sur lesquelles on a de moins en moins de contrôle démocratique ? Par exemple, il existe à présent une application qui permet de fusionner nos cartes de fidélité en une seule application. On souhaite alléger son portefeuille, mais on finit envahi de publicités… Typiquement, installer ce genre d'apps, c'est faire un gigantesque cadeau à Colruyt, Carrefour et d'autres, car cela les renseigne sur des tas de comportements, et cela leur permet de modifier leurs stratégies de négociation vis-à-vis de fournisseurs ou d'autres intermédiaires pour in fine maximiser toujours mieux leurs marges. Ceux qui détiennent les données et sont capables de les traiter sont en position de force par rapport aux producteurs et aux consommateurs. Est-ce ce monde-là qu'on veut ?
Il faut critiquer cette économie du Big Data, mais elle a pris une telle importance qu'on ne peut pas la critiquer sans y participer. Il faut pouvoir se doter d'outils qui permettent, avec les mêmes types d'algorithmes, de préparer des contre-feux.

Propos recueillis par
Monique Van Dieren et Guillaume Lohest

Le RGPD est-il réellement utile ou pas ? Ne manque-t-il pas sa cible, dans la mesure où les GAFA sont tout à fait capables, sans identification précise à une personne, de réaliser un profilage performant ?

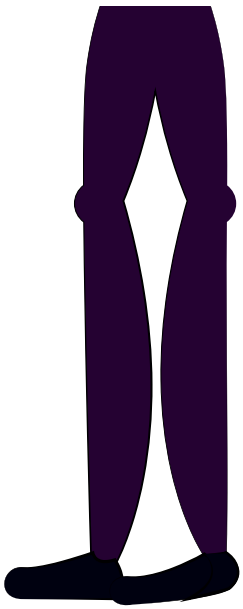
Bonne question ! Les GAFA se fichent totalement de la personne réelle qui est derrière un profil. De leur point de vue, vous êtes interchangeable, vous n'avez pas de nom. Néanmoins, le RGPD demeure important parce qu'il offre tout de même certaines garanties et protections. ***S'il ne servait à rien, le lobbying n'aurait pas été à ce point intense pour tenter de bloquer son adoption !***
Il protège en partie la vie privée des personnes. Mais en effet, ce n'est certainement pas la seule préoccupation en jeu, et ça ne règle rien par rapport au formatage des comportements.

Thomas Lemaigre



LES ALGORITHMES FORMATENT-ILS NOS GOÛTS ?

Lorsque nous écoutons de la musique sur Youtube ou sur Spotify, nous sommes assaillis de suggestions. Des playlists sont préétablies pour nous, sur base de ce que nous écoutons déjà et de ce que nos amis écoutent. Ce qui est incroyablement séduisant, c'est que ces propositions visent souvent très juste. Ce petit miracle est permis par l'amélioration permanente de ce qu'on appelle les *algorithmes de recommandation.*



Comment ça fonctionne ?

Ces algorithmes de recommandation, gigantesques formules mathématiques, prennent en compte une quantité de plus en plus impressionnante de données. Ils ne se limitent pas à proposer de la musique du même genre, mais affinent les recommandations sur base de différents mécanismes qui se complètent et s'enrichissent. Citons-en quatre :

- L'analyse de signal : sons, tempos, accords, timbres, etc.
- Le filtrage collaboratif : en résumé, si Jean aime Coldplay, que Jules aime Coldplay et aussi U2, alors il est probable que U2 plaira à Jean également.
- L'agrégation sociale ou *crowdsourcing*, qui permet de traduire en données utilisables l'analyse de millions de pages de sites spécialisés.
- Le filtrage basé sur le contenu, qui compare la liste de « tags » associés à l'utilisateur aux tags associés à des chansons, et fait émerger les contenus comprenant le plus grand nombre de correspondances.
- Enfin, le *deep learning* est l'automatisation et l'auto-amélioration de ces différentes méthodes intégrées. La machine s'entraîne et s'améliore elle-même sans aucun apport humain.

Quel est le souci au fond ?

Si les algorithmes de recommandation sont si efficaces pour anticiper ce que l'on aimera, nous allons leur faire de plus en plus confiance. Plus besoin de perdre du temps à lire des articles, à demander conseil, à chercher dans les rayons des médiathèques, à tester des artistes pour se rendre compte qu'on n'apprécie pas… Et nous resterons enfermés dans une bulle confortable correspondant à nos préférences. Quel est le problème ? La question se pose à un niveau philosophique ou existentiel. Souhaitons-nous vraiment faire l'économie des surprises, du hasard, des errements, des détours ? Souhaitons-nous vraiment que nos goûts restent enfermés en eux-mêmes ? N'y a-t-il pas aussi un ravissement irremplaçable à se laisser bousculer par tout autre chose ? N'est-ce pas d'ailleurs uniquement de cette façon que l'on *s'éduque* - étymologiquement, *sortir de soi-même* ?

Une vraie question de débat

Il y a matière à discuter des heures. Car ne soyons pas hypocrites : l'efficacité de ces algorithmes de recommandation est bluffante, et nous les utilisons massivement. Nous découvrons par là des tas de nouveaux contenus culturels que nous n'aurions sans doute pas découverts autrement. Notre bulle est certes réduite par les algorithmes, mais au sein d'une quantité immense de contenus culturels. Qu'en était-il avant ? Quel accès à la musique avait l'habitant d'un petit village en 1950, par exemple, par rapport à aujourd'hui ? N'étaient-ce pas d'autres bulles, physiques, sociologiques, qui limitaient l'accès à la culture ? Le pouvoir culturel des GAFA ne remplace-t-il pas celui des maisons de disque et des boîtes de production ?

Les questions sont réelles. Car les algorithmes n'influencent pas seulement la réception, mais aussi… la création. Va-t-on vers une création artistique de plus en plus convergente vers les formats les plus convoités ? Peut-on garantir par ailleurs que des acteurs culturels puissants ne bénéficient pas de « passe-droits algorithmiques », autrement dit que telle puissante maison de disque par exemple, ne paie Spotify ou Youtube pour apparaître plus souvent dans les recommandations ? Il est essentiel de comprendre comment ça fonctionne. Non seulement pour pouvoir « faire le mur » et s'enfuir occasionnellement de nos bulles culturelles, mais aussi pour être capable de mener un vrai débat collectif.

Guillaume Lohest

Pour aller plus loin

> Antoinette Rouvroy
> Philippe Vion-Dury
> Yves Citton
> http://sourdoreille.net/les-algorithmes-de-recommandations-nouvel-or-noir-des-services-de-streaming/
> http://maisouvaleweb.fr/les-algorithmes-nous-volent-notre-hasard-et-nous-nous-laissons-faire-une-conversation-avec-philippe-vion-dury/

COMMENT ÉVITER DE SE FAIRE DÉSHABILLER PAR GOOGLE & Cº ?

Vous n'avez pas envie que Google & Co connaissent le prénom de votre chat, vos préférences sexuelles ou le type de plante verte que vous affectionnez particulièrement ? Vous ne voulez pas qu'ils se fassent du fric sur votre dos ? Alors ces conseils sont pour vous. Loin de pouvoir vous rendre totalement invisible sur le net, voici quelques trucs et astuces pour limiter l'accès à votre vie privée.

Comment limiter mes traces sur Google ?

Après la page d'accueil, cliquez sur le menu qui se trouve à côté de « Mon activité ».

MAÎTRISER VOS DONNÉES

Vous pouvez **limiter la collecte de vos données personnelles** par Google : dans le menu, cliquez sur *Commandes relatives à l'activité*. Vous pourrez désactiver six éléments :

- L'activité sur le web et les applications utilisées
- L'historique des positions
- Les informations provenant de vos appareils (smartphones, tablettes, ordinateurs)
- L'activité vocale et audio
- Les vidéos regardées sur YouTube ainsi que votre historique des recherches sur la plateforme

DÉSACTIVER LA PUBLICITÉ PERSONNALISÉE

Google utilise vos données à des fins publicitaires mais vous pouvez diminuer le nombre de données que vous livrez au moteur de recherche en refusant de recevoir des publicités personnalisées. Vous pouvez limiter la collecte de ces données en cliquant dans le menu sur Autres activités Google puis sur Paramètres des annonces et là, vous pourrez **désactiver** l'option.

Vous pouvez **effacer** (partiellement ou complètement) **les données personnelles archivées par Google**. Dans le menu, cliquez sur *Supprimer des activités.*

CONSULTER VOS DONNÉES

Vous pouvez consulter les **données collectées par Google** en vous rendant sur **myactivity.google.com**. Il vous suffira de vous connecter à votre compte Google. Vous y trouverez le type d'appareil avec lequel vous vous connectez, le type de navigateur, les applis et les sites consultés, les données issues de Google Maps, vos recherches sur Google mais aussi sur YouTube, les applications que vous utilisez avec votre téléphone…

Pour consulter l'**historique de vos trajets**, cliquez sur le menu et sur *Autre activité Google* puis sur *Historique des positions*. Vous pourrez découvrir jour par jour, la carte des trajets que vous avez empruntés ainsi que les commerces qui se trouvaient sur votre chemin. Si « aucun lieu visité » est affiché, cela signifie que la localisation par Google était déjà désactivée.

Comment limiter mes traces sur Internet ?

COOKIES

Supprimez les cookies de votre navigateur web (Chrome, internet explorer, Mozilla Firefox). Tous les navigateurs vous permettent de configurer le blocage des cookies. Cela peut rendre la navigation moins aisée, voire rendre impossible l'accessibilité à certaines fonctions des sites. Attention, il est conseillé de n'accepter que les cookies des sites web dont vous autorisez qu'ils collectent vos informations de navigation.

HISTORIQUE ET FICHIERS EN CACHE

Supprimez votre historique de recherche via votre navigateur web. Il est possible d'activer par défaut « Effacer l'historique de navigation en quittant le navigateur ».

NAVIGATION PRIVÉE

Cette option à activer sur votre navigateur web (Chrome, internet explorer, Mozilla Firefox) permet d'éviter la collecte de vos données de navigation. Par exemple pour Mozilla, cliquez sur le « menu » puis sur « nouvelle fenêtre de navigation privée ».

CRYPTAGE DES DONNÉES

Il existe des logiciels gratuits qui permettent de crypter vos données mais aussi de protéger votre anonymat sur la toile. Exemple : le réseau Thor qui brouille votre adresse IP et crypte vos données ou AxCrypt.

ADRESSES MAILS

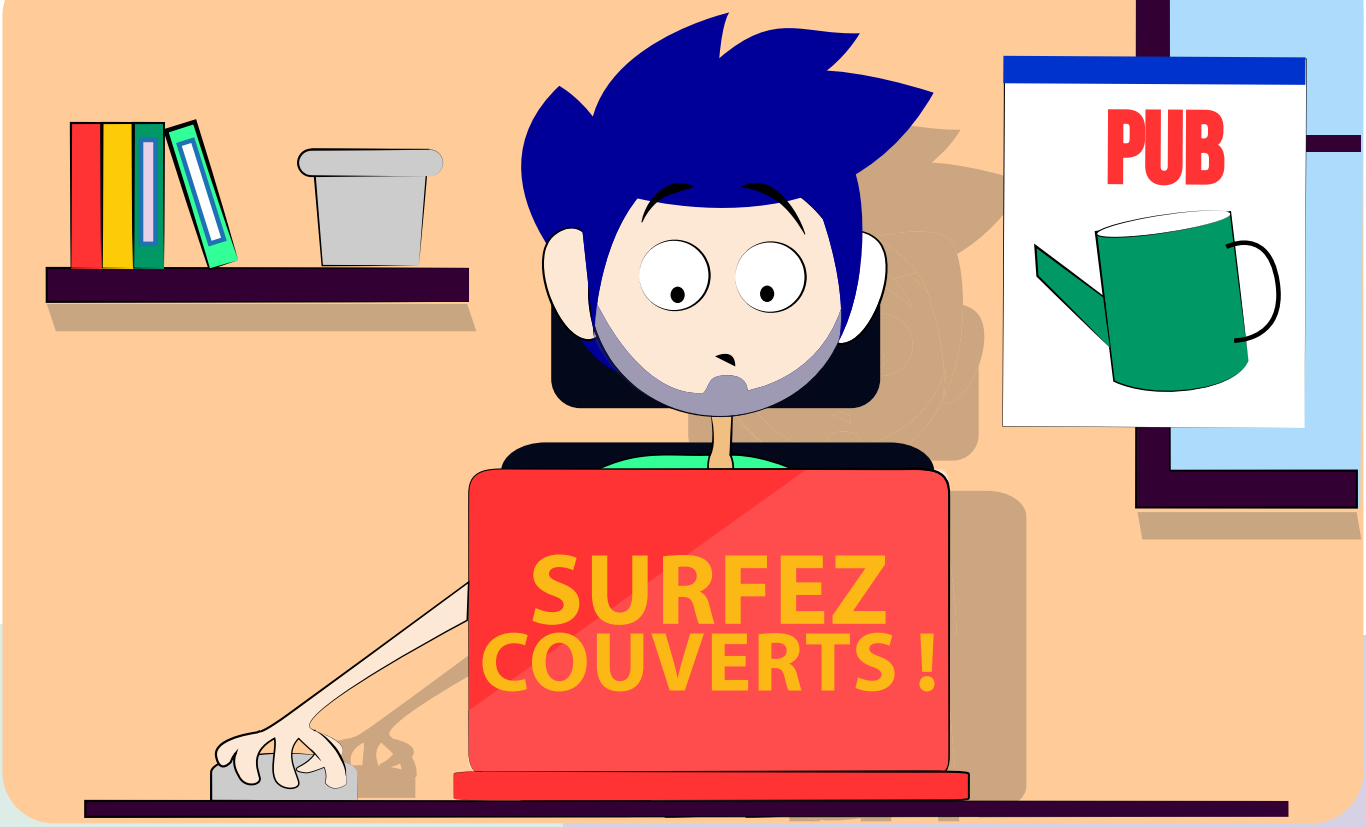
Disposez d'au moins deux adresses mail : une que vous utilisez à des fins de loisirs (concours, inscription à des forums de discussion, à des sites de rencontre…) et une autre à des fins plus personnelles (factures, achats en ligne…). Changez régulièrement de mot de passe. Attention les boites mails gratuites permettent en contrepartie aux sociétés qui les gèrent d'accéder au contenu et d'adapter ainsi l'offre publicitaire. Supprimer régulièrement vos mails (ainsi que le dossier éléments supprimés) afin de limiter vos traces.

MOTEURS DE RECHERCHE

Ils gardent une trace de toutes les recherches que vous effectuez. Utilisez des moteurs de recherche alternatifs à Google qui ne collectent pas vos données personnelles : Start page, duckduckgo

ADRESSE IP

Des serveurs proxy vous permettent de masquer l'adresse IP, le n° d'identification de votre appareil, lorsque vous consultez un site. Vous pouvez utiliser par exemple le serveur proxy www.proxify.com



Comment limiter mes traces sur Facebook ?

MAÎTRISER VOS DONNÉES

A partir de votre compte Facebook, accédez à vos paramètres. Vous pourrez gérer :

- La **confidentialité** de votre compte : qui peut voir quoi sur votre journal, qui peut vous identifier.
- La **localisation** : désactivez la localisation, supprimez votre historique en cliquant sur l'option.
- La **reconnaissance faciale** si vous ne souhaitez pas être reconnu dans les photos et/ou vidéos.
- Les **applications** qui transmettent des informations à Facebook et le cas échéant supprimer celles que vous n'utilisez plus.
- Les **jeux** : supprimer ceux que vous n'utilisez plus et de manière générale, évitez d'utiliser les jeux sur Facebook qui sont de grands collecteurs de données personnelles (accès à votre profil, photo de couverture, genre, nom et prénom…).
- Les **publicités** : vous pourrez désactiver toutes les options concernant les **publicités** notamment l'usage de certaines de vos données personnelles (centres d'intérêts, situation amoureuse, employeur, fonction, scolarité) par les annonceurs.

CONSULTER VOS DONNÉES ET LES TÉLÉCHARGER

« **Paramètres généraux** » -> « ***Vos informations personnelles*** » pour la version PC ou « ***Vos informations Facebook*** » -> « ***Accéder à vos informations*** » pour la version smartphone. Vous pouvez également les télécharger. Vous recevrez un mail avec un dossier qui contient toutes les informations que Facebook possède sur vous. Ce qui est intéressant dans cette démarche, c'est la prise de conscience de la quantité de données que nous laissons derrière nous qui nous poussera peut-être à mieux les protéger.

Conseils BONUS

DÉSACTIVER LES APPLIS EN ARRIÈRE-PLAN SUR VOTRE SMARTPHONE

Celles-ci continuent à collecter des données alors que vous n'êtes pas en train de les utiliser.

SUPPRIMEZ LES APPLICATIONS QUE VOUS N'UTILISEZ PLUS

Ce n'est pas parce que vous supprimez les raccourcis de vos applis qui se trouvent sur votre écran d'accueil que votre compte l'est également. A partir de l'appli, demandez la suppression de votre compte et le cas échéant, à la firme de supprimer vos données personnelles.

DONNÉES DE LOCALISATION

Désactivez ces données à partir des paramètres de votre téléphone. Désactivez le bouton de géolocalisation, le wifi, le Bluetooth, les données mobiles quand vous n'en n'avez pas besoin.

CONNECTION VIA LE BOUTON FACEBOOK

Évitez de vous connecter à vos applications via le bouton Facebook. Il est préférable que vous encodiez à chaque connexion vos identifiants et mot de passe.

De manière générale, déconnectez-vous de chaque session lorsque vous êtes par exemple sur un site de commerce ou si vous allez sur Facebook. N'oubliez pas que vous avez une responsabilité envers vos amis : même si vous vous fichez que l'on collecte des éléments sur vous, via votre profil on pourra accéder à des informations concernant vos proches : par exemple, lorsque vous acceptez qu'une appli ait accès à votre répertoire téléphonique, cela donne accès au n° de téléphone de personnes qui ne sont peut-être pas d'accord de figurer dans une base de données.

Si tous ces conseils vous donnent le tournis, vous pouvez adopter une solution plus radicale, vous pouvez toujours exploser votre smartphone sur le sol ! Mais si vous tenez malgré tout à votre téléphone mobile… venez à nos **Cryptopartys** avec vos écrans et on vous livrera quelques astuces, promis ! - **Infos en page 24**

Claudia Benedetto

IMPUISSANTS FACE AUX GAFA ?

Quelques propositions à défendre, et des idées à mettre en chantier

LES SERVICES PUBLICS DOIVENT MONTRER L'EXEMPLE

Le gouvernement fédéral a autorisé en catimini durant les congés d'été la création d'une méga Data Warehouse, une base de données géante qui regroupe toutes les informations déjà enregistrées dans les différents services de l'Etat.

Elle a certes un intérêt en termes d'amélioration des statistiques belges, mais elle cache en réalité un autre objectif, celui de détecter, à partir d'une foule d'informations, les risques de travail au noir et de fraude sociale. Bien qu'étant un puissant outil de profilage des personnes, aucun encadrement légal ni contrôle parlementaire ne règlemente le système Oasis.

- Nous devons exiger un contrôle démocratique sur les finalités ainsi que sur les méthodes de collecte et d'utilisation de cette gigantesque banque de données.

QUELQUES AUTRES PROPOSITIONS

- Demander aux pouvoirs publics de promouvoir et d'utiliser des logiciels et des moteurs de recherche qui ne captent pas les données personnelles (exemple : Qwant).
- Interdire l'utilisation parfois sournoise des réseaux sociaux dans le but de conditionner des droits (ex : consultations des pages Facebook par les CPAS ou par le Fisc…).
- Sur des sites d'intérêt public, l'accès à l'information ne doit pas être conditionné par des cookies.
- Proximus, entreprise publique autonome, ne devrait pas être autorisée à utiliser une application telle que *My Analytics*, qui suit la localisation des abonnés grâce à leur carte SIM, à leur insu, et les vend ensuite (dépersonnalisées) à des sociétés privées.

FAIRE APPLIQUER ET AMÉLIORER LE RGPD

Le RGPD est une avancée importante en matière de protection des données personnelles. Mais pour que cette avancée soit effective, il faut :

- Veiller au contrôle de son application par l'Autorité de protection des données, en particulier en ce qui concerne les réseaux sociaux et les services dérivés (applications…). Et que le contrôle soit assorti de sanctions proportionnelles à leur chiffre d'affaires. Or, l'application de sanctions et le montant de celles-ci restent un élément flou de ce nouveau RGPD.
- Préciser certains aspects du règlement qui laissent encore la porte ouverte à des interprétations défavorables au consommateur, notamment en matière d'effacement, de minimalisation et de portabilité des données. (Voir p. 10)

RÈGLEMENTER DAVANTAGE L'USAGE DES COOKIES

Avec la géolocalisation, les cookies sont une mine d'or en matière de collecte de données personnelles. Or, il est très difficile d'y échapper.

- Soutenir, au niveau européen, une nouvelle proposition de directive (Dir. Vie privée et communications électroniques[1]) qui règlemente davantage l'utilisation des cookies par des entreprises tierces, une des principales sources de récolte des données personnelles. La partie n'est pas gagnée car les entreprises spécialisées en marketing direct font un lobbying intense contre cette proposition.

1. Proposition publiée le 10 janvier 2017, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52017PC0010&from=EN

MIEUX ENCADRER LES TECHNIQUES DE GÉOLOCALISATION

Les méthodes de géolocalisation sont multiples et souvent méconnues des utilisateurs de smartphone. Certaines d'entre elles sont insidieusement installées.

- Obliger les fabricants de smartphone à prévoir plus clairement les procédures d'acceptation ou de refus des méthodes de géolocalisation.
- Donner davantage d'information sur les finalités pour lesquelles les données sont récoltées et les conséquences si on refuse la collecte des données.
- Saisir l'Autorité de protection des données pour qu'elle limite l'utilisation des systèmes "Indoor" de géolocalisation (balises installées dans les commerces par exemple), comme cela a été imposé aux Pays-Bas sur base des principes prônés par le RGPD.
- Selon le principe de "minimalisation des données", ne pas obliger le consommateur à accepter la géolocalisation pour télécharger des applications qui ne nécessitent pas d'être géolocalisées pour fonctionner.
- Le consentement du consommateur doit être donné quelle que soit la méthode de géolocalisation (Wifi, 4G, Bluetooth) et ne doit pas se faire "par défaut".

INFORMER SUR L'UTILISATION ET LA VALEUR DES DONNÉES

Le business model des GAFA (et de nombreuses autres entreprises, notamment européennes) est basé sur la commercialisation de nos données personnelles. Même si le RGPD a mis un peu d'ordre dans les règles de collecte et de traitement des données, cela n'empêche pas ces entreprises de vendre nos données en fournissant le moins d'information possible sur la valeur de ces données et ce qu'ils en font, la plupart du temps sans notre consentement.

- **Les organisations de consommateurs demandent qu'un cadre légal soit déterminé pour avoir accès à l'information sur la valeur des données.**

Au niveau européen, le COFACE[1] émet une proposition qui mérite d'être étudiée : la définition d'indicateurs qui aideraient les consommateurs dans leurs choix d'utiliser tel ou tel service de téléphonie mobile ou internet. Quelques indicateurs possibles : les montants générés par l'utilisation des données personnelles, le rapport entre les données collectées et le produit vendu, dans quelle mesure les données sont utilisées à des fins de marketing…

L'objectif de ce type de démarche ne doit selon nous pas être de "monétariser" nos données personnelles (proposition que nous ne soutenons pas), mais de sensibiliser à l'usage qui en est fait, et d'aider les consommateurs dans leurs choix de services ou d'opérateurs.

Cette proposition mérite que l'on s'y attarde. Dans le cas de la création de normes ou d'un label, cette initiative peut être lancée par les organisations de consommateurs mais devra obtenir l'aval de l'industrie du numérique, ce qui n'est pas gagné d'avance. Mais rien n'empêche la Belgique d'adapter déjà sa législation en ce sens.

(1) Coface « current challenges and impact on the digitalisation on families » http://www.coface-eu.org/wp-content/uploads/2017/09/COFACE-policy-briefing-2016-Digital-Economy.pdf

LUTTER CONTRE LE MONOPOLE DES GAFA

L'arsenal législatif européen commence à se réveiller pour faire barrage au monopole des GAFA, qui est déjà néfaste pour la protection des consommateurs et de la vie privée.

Google vient par exemple de se voir infliger une amende de 3,4 milliards € parce qu'il a imposé son système Androïd (et toutes les applications qui y sont liées) à tous les utilisateurs de smartphone. Il est urgent d'agir maintenant pour que ces géants ne s'emparent pas complètement de domaines majeurs tels que la santé, la gestion de l'espace…

Pour Arno Pons, du Think Tank français Digital New deal[1], les Big Tech se comportent comme Poutine : plus elles ont du pouvoir, plus elles en abusent. Une fois qu'elles ont le monopole, elles changent les règles du jeu et les imposent.

- **Il faut condamner ces pratiques et encourager la Commission européenne à lutter contre les monopoles.**
- **L'Europe devrait jouer un rôle moteur dans le soutien à des initiatives émergentes dont le modèle économique n'est pas basé sur la monétarisation des données personnelles.**

1. Interrogé par C. Charlot dans Trends-Tendances du 26.07.18.

LUTTER CONTRE L'ÉVASION FISCALE À GRANDE ÉCHELLE DES GAFA

Les géants du numérique sont les champions des montages fiscaux qui leur permettent de payer le moins possible d'impôts et leur siège social est installé dans des pays où la fiscalité est plus avantageuse (par ex. en Irlande). Un exemple : *Amazon*, qui n'a pas d'entité juridique en Belgique, a généré un chiffre d'affaires estimé à un milliard € en 2016 sur notre territoire et a payé … 0 € d'impôt !

Le Réseau pour la Justice fiscale fait de nombreuses propositions pour une harmonisation fiscale au niveau européen, pour stopper l'évasion fiscale ainsi que les montages financiers qui permettent aux multinationales (dont les géants du Net) d'échapper quasi totalement à l'impôt.

UNE TAXE GAFA SUR LA COMMERCIALISATION DES DONNÉES

Selon le cabinet d'étude IDC (International Data Corporation), le marché des données personnelles des citoyens/consommateurs des 28 pays de l'UE représentait 300 milliards € en 2016 (perspective : 430 milliards en 2020). Une somme colossale qui est constituée en grande partie grâce à la collecte et à la vente de nos données personnelles.

En attendant une réforme globale de la fiscalité, la Commission européenne a proposé en mars dernier une taxe sur les GAFA de 3% sur les revenus de la vente de publicités et de données des géants du Net. Elle concernerait environ 150 entreprises dans l'UE et pourrait rapporter 5 milliards. Certains pays de l'Union européenne tentent de s'y opposer, d'autres ne sont pas très chauds.

Faisons pression sur notre gouvernement pour qu'il appuie cette proposition !

Contrairement au principe de récupération individuelle de la valeur des données (voir p. 21), une telle taxe pourrait bénéficier à la collectivité en finançant par exemple la presse écrite et audiovisuelle mise à mal par la concurrence des réseaux sociaux. C'est peut-être de l'ordre de l'utopie, mais cela s'inscrit dans une certaine tradition européenne de gestion des communs comme les droits d'auteurs, les données de santé, etc. Un peu à l'image de la *Taxe Tobin* sur la spéculation financière qui était censée contribuer au financement du développement.

Monique Van Dieren

Interview-minute

« ON PEUT BOUSILLER LEUR BUSINESS MODEL ! »

PHILIPPE LAMBERTS, co-président du groupe des Verts au Parlement européen, n'a pas sa langue en poche. Nous lui avons demandé ce qui peut, selon lui, contrecarrer la toute-puissance des géants du Net.

Google, Amazon, Facebook, Apple, Microsoft sont tous américains. Ils imposent leur business model partout dans le monde et en particulier en Europe, et sont en situation de quasi monopole. Sont-ils inattaquables ?

L'Europe pourrait avoir une prise sur certaines d'entre elles. Rompre le monopole d'Amazon, ça ne doit pas être très compliqué s'il y a une volonté politique. De toute manière, on va sans doute bientôt voir débarquer en Europe d'autres plateformes géantes de vente en ligne telles que la chinoise Alibaba.

Par contre, pour Google ou Facebook, ce sont des monopoles naturels. Ces entreprises n'étant pas européennes, l'Europe ne peut pas décider seule de l'avenir de ce genre de monopole. Par contre, on doit être capable de contrôler ce qu'ils font et de leur imposer des obligations s'ils veulent opérer en Europe. Des obligations fiscales, d'abord ; taxer leurs revenus publicitaires, taxer l'usage des données, taxer leurs bénéfices en fonction du nombre d'utilisateurs qu'ils ont en Europe. Ce n'est pas très compliqué.

On peut également leur imposer des obligations en matière d'utilisation des données personnelles. Ou encore -c'est une question de volonté politique- les obliger à offrir le modèle payant. Le principe serait le suivant : comme utilisateur, soit vous utilisez la plateforme gratuitement et vous savez que le prix à payer, c'est l'utilisation de vos données personnelles à des fins commerciales. Soit vous êtes prêts à payer un prix d'usage annuel, qui peut être très bas (1 ou 2 € par mois) car au final, les revenus publicitaires par utilisateur sont assez faibles.

On pourrait leur imposer d'offrir ce choix à l'utilisateur. Contrairement à ce que prône Test-Achats, il ne s'agit pas de demander aux GAFA de nous rétribuer pour utiliser nos données, c'est la démarche inverse : c'est nous qui rétribuerions Facebook afin qu'il n'utilise pas nos données personnelles. Je trouve que cette option devrait être encouragée. Tout d'abord, parce que la gratuité de l'information et des services, ça n'existe pas et ça n'a jamais existé. Ensuite, parce qu'on peut bousiller le business model des GAFA en restreignant fortement l'utilisation de nos données personnelles. Du coup, ils n'auraient plus rien à vendre aux annonceurs publicitaires ! Pour moi, le vrai levier d'action qu'on a sur les GAFA, c'est celui-là.

Même si l'Europe encadre davantage l'utilisation des données que les Etats-Unis (voir le RGPD), on a pourtant l'impression qu'elle laisse tranquillement les GAFA installer leur business model chez nous. Pourquoi ?

Certains pays de l'Union européenne ont peur de se fâcher avec les Etats-Unis, mais pas tous. Clairement, beaucoup d'initiatives de la Commissaire à la Concurrence Margrethe Vestager ciblent les GAFA, en particulier Facebook et Google ; elle n'a pas froid aux yeux ! Mais c'est vrai qu'il y a une forme d'aveuglement face aux progrès technologiques. Je le constate dans les cercles de décision européens ; on continue à dire que c'est formidable, ces nouveaux business models, au lieu de penser à brider la collecte de nos données.
Le vrai problème des GAFA se situe du côté des réseaux sociaux : plus il y a d'utilisateurs, plus le réseau a de la valeur pour l'utilisateur. C'est en cela que je dis que Facebook est un monopole naturel ! Il faut aller voir du côté de ce que certains économistes comme Elinor Ostrom ont produit sur la gouvernance des Communs. Ils montrent que les seules alternatives, ce n'est pas obligatoirement devoir choisir entre le privé ou le public.

Si je dis ça c'est parce que pour moi, Facebook est devenu un Commun. Je préfèrerais éliminer la publicité de Facebook, mais on n'est pas obligé de le nationaliser pour autant ! Avez-vous envie de donner à l'Etat la propriété de la plateforme sur laquelle les gens partagent tant de choses de leur vie privée ? Moi pas. Je ne veux la donner ni à l'Etat, ni à une entreprise privée. Je veux que ça puisse être gouverné comme un Commun. Je crois qu'il y a un vrai travail à faire dans ce sens. On pourrait dire à Facebook que nos conditions pour qu'il puisse opérer en Europe, c'est d'accepter de se défaire de la gouvernance du Commun. Il y a des choses à réfléchir dans ce sens, mais on en est encore bien loin...

Vous êtes co-président du groupe des Verts au Parlement européen. Y a-t-il dans vos cartons un projet de taxation sur le commerce des données ?

Le Parlement européen n'a pas autorité pour le faire. Mais différentes pistes sont sur la table, par exemple taxer le flux des données ou les recettes publicitaires. Par contre, sur la taxation de leurs profits, le projet d'assiette commune et consolidée sur l'impôt des sociétés règlerait le problème de la taxation des GAFA. IIW est urgent que l'ISOC soit harmonisé au niveau européen.

Propos recueillis par Monique Van Dieren

RÉCUPÉRER LA VALEUR DE NOS DONNÉES PERSONNELLES ?

La gigantesque masse de données que nous fournissons aux GAFA est utilisée par ces multinationales pour gagner de l'argent. Comment ? En les vendant à des fins publicitaires. L'ensemble de ces données, agrégées massivement, traitées par des algorithmes, permettent un ciblage des publicités qui vaut cher pour n'importe quelle entreprise. Les données personnelles ont donc une valeur commerciale. On estime que l'ensemble du marché des données en Europe pourrait peser environ 1.000 milliards d'euros en 2020.

Il est fréquent de considérer que cette cession de nos données est, en quelque sorte, la contrepartie logique de la gratuité des innombrables services que nous offrent Google, Facebook, Apple, Amazon. Nous payons ces services sous forme de données personnelles. Mais le deal est-il équitable ? Ne faut-il pas récupérer une partie de cette valeur ? Et si oui, comment ? Voici les réponses qui correspondent à des philosophies différentes.

- **Selon une approche libérale**, les individus devraient pouvoir gérer eux-mêmes la vente de leurs données. Le think tank ***Génération Libre***, en France, défend la création d'un droit de propriété individuel sur les données personnelles. Cela permettrait aux utilisateurs de contractualiser, de monétiser leurs données, pour les vendre ou, au contraire, pour payer le prix des services fournis par les GAFA en échange d'une non-utilisation des données personnelles.

- **Dans une approche similaire, *Test-Achats***, en Belgique, mène actuellement une action collective contre Facebook : avec ses organisations sœurs italienne, portugaise et espagnole, elle réclame 200 euros de dommage pour tous les utilisateurs, pour l'utilisation abusive de données révélée par le scandale *Cambridge Analytica*. Il s'agit ici d'une campagne ponctuelle, visant une rétribution individuelle. Selon La Libre en ligne, 19.500 personnes s'y sont inscrites.

- **Toujours dans une logique de choix individuel**, une quatrième approche est d'obliger les GAFA à laisser aux utilisateurs le choix de payer une redevance d'utilisation, avec à la clé l'interdiction de capter nos données personnelles. A l'inverse de Test-Achats, il ne s'agit donc pas de demander une compensation financière aux GAFA parce qu'ils utilisent nos données, mais bien de les payer pour qu'ils n'utilisent ou ne vendent pas nos données

- Certains s'inquiètent de ces perspectives de commercialisation individuelle des données, défendant plutôt la **protection de la vie privée** plutôt que sa marchandisation. C'est cette philosophie qui préside au récent règlement européen de protection des données (RGPD).

- Enfin, pourrait exister une **revendication plus collective** : une taxation des GAFA afin de socialiser la richesse récupérée. La manière de redistribuer cette richesse peut varier d'une approche à l'autre. Cela peut prendre la forme d'une rétribution directe des citoyens ou plutôt d'investissements collectifs.

Ces différentes options soulèvent des débats de société importants. Aux Équipes Populaires, nous nous situons évidemment dans une tradition de protection par le droit et de gestion collective de la richesse créée. Il ne nous semble ni souhaitable ni possible que chacun devienne le petit entrepreneur de ses données personnelles. Cela augmenterait encore davantage les inégalités. À ce stade néanmoins, vu la complexité du sujet et des enjeux économiques, il serait aventureux d'avancer des chiffres précis.

Guillaume Lohest

CRYPTOPARTY

Apprendre à crypter ses données, limiter ses traces sur internet

Tables de discussion

Ateliers techniques

Bar avec petite restauration

Atelier créatif

Une campagne de sensibilisation des Equipes Populaires

ep Equipes Populaires

Avec le soutien de FÉDÉRATION WALLONIE-BRUXELLES

SURFEZ COUVERTS !

Une campagne de sensibilisation des Equipes Populaires

ep

www.equipespopulaires.be

Avec le soutien de FÉDÉRATION WALLONIE-BRUXELLES

SURFEZ COUVERTS !

Google, Amazon, Facebook, Apple… Les Géants du Net nous connaissent mieux que notre meilleur ami ou notre partenaire !

Nos données personnelles sont une mine d'or pour les GAFA: adresse mail, géolocalisation, achats en ligne, photos et coordonnées de nos amis… Ils ne se gênent pas pour utiliser notre vie privée à des fins commerciales. Un business très juteux qui pose question, tant en termes de protection de la vie privée que de formatage de nos modes de vie et de consommation.

Comment limiter nos traces sur internet, reprendre la maîtrise de nos données personnelles ? Comment reprendre du pouvoir sur ce modèle économique qui nous est de plus en plus imposé ? Et la démocratie dans tout ça ?

Résister à la surpuissance des Géants du Net, c'est possible… Parlons-en !

Dossier d'information et programme des activités sur www.equipespopulaires.be

Une campagne de sensibilisation des Equipes Populaires

CRYPTOPARTY

Apprendre à crypter ses données, limiter ses traces sur internet

Ateliers techniques

- *Consulter et effacer ses données personnelles*
- *Utiliser des logiciels de cryptage*
- *Limiter ses données de géolocalisation*

Tables de discussion

- *Que fait-on avec mes données personnelles ?*
- *Comment les GAFA s'enrichissent sur notre dos ?*
- *Rien à cacher… vraiment ?*

Liège - Vendredi 16 novembre
De 17h30 à 22h à **La Zone**
Quai de l'Ourthe, 42
Infos : 0494/12.91.73 ou 0485/16.26.45

Bruxelles - Vendredi 23 novembre
De 18h à 21h30 à **l'Ades'if**
Rue de Liedekerke, 71
(St Josse)
Infos : 0487/70.43.36

Charleroi - Mardi 20 novembre
De 15h30 à 18h30
à la **Brasserie de l'Eden**
Bd Jacques Bertrand,1
Infos : 0496/11.78.47

Namur - Samedi 24 novembre
De 17h à 21h
au **Projet 42**
Rue Bas de la place, 17
Infos : 0488/47.66.15

Organisation : **Equipes Populaires**
www.equipespopulaires.be