Le Bulletin de santé d'Internet 2019 constitue une compilation d'études et présente les éléments qui participent au développement d'Internet et ceux qui lui nuise, selon cinq thèmes.

mzl.la/ihr-fr

04 Readme

2019 Enjeux

06 Exigeons davantage de l'intelligence artificielle
11 Réinventer la publicité numérique
16 Le pouvoir des villes

Vie privée et sécurité

21 Un espace sûr ?

Ouverture

35 Ouvert, jusqu'à quel point ?

Inclusion numérique

48 Qui est le bienvenu en ligne ?

Éducation à Internet

61 Vers une égalité des chances ?

Décentralisation

74 Qui contrôle Internet ?

Participer

89 10 minutes pour un Internet plus sain
90 Rejoindre le mouvement

Readme

Internet se porte-t-il mal ? Nous avons semé cette interrogation dans votre esprit avec le titre de ce rapport et les questions qu'il pose. Cependant, nous n'y répondrons pas par un simple oui ou non.

En effet, comme vous l'avez peut-être compris, cette publication ne représente ni un classement par pays ni un compte à rebours alarmiste. Nous vous invitons à évaluer avec nous à quoi tient la bonne santé d'Internet et à participer à l'établissement d'un programme qui nous permettra de travailler ensemble pour créer un Internet véritablement centré sur l'humain.

Avec cette compilation d'articles, d'entretiens et d'analyses (conçue avec l'aide de centaines de lecteurs, en collaboration avec plus de 200 experts), nous aspirons à montrer que si les conséquences mondiales d'une mauvaise utilisation d'Internet peuvent être considérables – pour la paix et la sécurité, pour les libertés politiques et individuelles, pour l'égalité humaine -, aucun problème n'est réellement irrémédiable. Davantage de personnes que vous ne l'imaginez œuvrent à faire d'Internet un espace plus sain et agissent dans ce sens en consacrant leurs compétences, leur créativité et même leur courage à leur entreprise, à la technologie, au militantisme, aux politiques et à la réglementation, à l'éducation ainsi qu'au développement communautaire.

Ce rapport annuel représente un appel à l'action pour reconnaître les éléments qui ont une incidence sur Internet aujourd'hui grâce à la recherche et à l'analyse, et pour adopter l'idée que nous, en tant qu'humains, pouvons changer la façon dont nous gagnons de l'argent, gouvernons les sociétés et interagissons les uns avec les autres en ligne.

Si expliquer comment améliorer l'état de santé d'Internet n'est pas aisé, cela tient en partie au fait que beaucoup d'éléments problématiques passent inaperçus. En tant qu'internautes, nous avons tendance à ne pas penser aux câbles à fibres optiques qui passent sous les océans, ni aux hommes et aux femmes qui assemblent nos dispositifs électroniques et encore moins aux processus de décision codés dans des appareils « intelligents ». Beaucoup d'entre nous ne savent pas comment nos sociétés Internet préférées réalisent leurs bénéfices ou comment nos désirs personnels et nos traits de caractère sont identifiés au long de notre vie.

Pour être tout à fait honnêtes, beaucoup d'entre nous préféreraient probablement ne pas savoir. Pourquoi gâcher la magie de la gratification instantanée obtenue lorsque nous appuyons sur un bouton, qui cache tous les processus technologiques appliqués en arrière-plan. L'inconvénient, c'est que souvent nous n'identifions pas les besoins de changement systémique avant que les problèmes fassent la Une. Nous préférons imaginer que nous sommes protégés : par des sociétés Internet de pointe, par les gouvernements, par d'autres utilisateurs plus avisés.

Nous faisons sans arrêt des choix au sujet des logiciels à utiliser, des risques de sécurité à prendre ou des mesures à adopter pour protéger la vie privée de nos enfants et de nos proches. En tant que défenseurs d'un Internet plus sain, l'heure est venue d'opérer de

meilleurs choix. Luttons pour corriger ce qui ne va pas et joignons nos efforts pour prendre la bonne voie. À la lecture du Bulletin de santé d'Internet, jetons un coup d'œil aux possibilités connues et insoupçonnées d'Internet et considérons cet écosystème riche, diversifié et complexe comme un écosystème qui s'adapte à nos actions collectives et évolue au fil du temps.

Les enjeux analysés cette année vous invitent à réfléchir à trois sujets qui, chacun à sa manière, se « cachent juste sous nos yeux » et méritent une attention particulière pour améliorer la santé d'Internet.

Nos sociétés et nos économies vont bientôt connaître des transformations profondes en raison des capacités croissantes d'apprentissage et de prises de décisions des machines. Comment commencer à imposer des exigences plus strictes relatives au développement de l'intelligence artificielle pour que cette technologie répondent à nos besoins ?

Vous avez sûrement entendu que les publicités ciblées et la collecte de données personnelles se trouvent au cœur d'une multitude de dysfonctionnements liés à Internet. Quels sont les efforts prometteurs pour redresser la situation ?

Plus de la moitié de la population mondiale vit actuellement en ville. Croyez bien que les autorités sont confrontées à des défis difficiles (et à des intérêts divergents) lorsqu'il s'agit de réaliser nos idéaux pour un Internet plus sain. Non, il ne s'agit pas de « villes intelligentes », mais du pouvoir inexploité des gouvernements municipaux et de la société civile à collaborer pour améliorer la santé d'Internet dans le monde entier.

Remerciements

Un grand nombre de chercheurs, de boursiers, de rédacteurs et de partenaires de Mozilla ont généreusement contribué à ce rapport avec des données et des idées, tout comme d'innombrables lecteurs.

Consultez ci-dessous la liste complète des contributeurs.

Éditrice: Solana Larsen
Cheffe de projet: Kasia Odrozek
Chargé de diffusion: Jairus Khan
Analyste de recherche et de données: Stefan Baack
Assistante d'édition: Eeva Moore

Contactez-nous:
internethealth@mozillafoundation.org

Pour les demandes des médias, consultez la page:
internethealthreport.org/press

L'identité visuelle et le code proviennent de Rainbow Unicorn, un studio de création et une agence numérique berlinoise. Christian Laesser a réalisé les visualisations de données et Julian Braun les créations 3D. La totalité du rapport sera traduit par Global Voices de l'anglais vers le français, l'espagnol et l'allemand (avec des dates de lancement échelonnées).

Ouverture Enjeux

Exigeons davantage de l'intelligence artificielle

Stefania Druga enseigne aux enfants la programmation en intelligence artificielle.

Dans le cadre de ses recherches, elle a étudié comment 450 enfants de sept pays perçoivent et interagissent avec des jouets et des assistants virtuels connectés, comme Amazon Alexa ou Google Home.

Les enfants ont les capacités de comprendre bien plus que ce qu'imaginent les parents, indique-t-elle, y compris que l'apprentissage automatique des machines dépend des données disponibles pour leur entraînement.

La philosophie derrière le logiciel qu'elle a développé pour l'enseignement considère que si nous offrons aux enfants la possibilité de jouer un véritable rôle dans leurs relations avec les technologies « intelligentes », ils peuvent décider activement du comportement qu'ils souhaitent les voir adopter. Les enfants recueillent des données et instruisent leur ordinateur.

Une approche similaire, simple : voilà ce qui devrait de toute urgence s'appliquer à d'autres domaines de la société.

Pour saisir les implications de l'intelligence artificielle pour l'humanité, nous devons la comprendre, puis décider ce que nous voulons qu'elle réalise. Son utilisation augmente à une vitesse vertigineuse (aussi bien à des fins de divertissement, que de gouvernance ou dans les activités militaires ou commerciales).Pourtant, les risques connexes ne sont certainement pas suffisamment étudiés.

« Oui, il s'agit probablement d' intelligence artificielle », est la réponse simple et courte de la journaliste Karen Hao, spécialiste de l'intelligence artificielle, à propos de toute technologie capable d'écouter, de parler, de lire, de bouger et de raisonner. Sans nécessairement s'en rendre compte, tous les internautes interagissent déjà avec une certaine forme d'intelligence artificielle.

Schématiquement, l'apprentissage automatique et les intelligences artificielles représentent simplement la prochaine génération de l'informatique. Ces technologies rendent possible un niveau bien supérieur d'automatisation, de prédiction et de personnalisation.

En outre, elles constituent un changement si fondamental dans les possibilités offertes par les ordinateurs en réseau que nous pouvons imaginer qu'elles occuperont bientôt une place bien plus importante dans notre vie.

Qu'il s'agisse des résultats des moteurs de recherche, des listes de lecture musicales ou d'itinéraires de navigation, ces services ne reposent pas sur la magie. Des spécialistes codent des algorithmes, à savoir des formules qui décident comment les décisions doivent être automatisées en fonction des données qui leur sont fournies.

Le sentiment de magie commence lorsque la technologie ouvre de nouvelles possibilités. This Person Does Not Exist représente un bon exemple. Consultez le site et actualisez la page pour voir s'afficher une infinité de visages de personnes qui n'existent pas. Ces images, inspirées par une base de données de visages de personnes bien réelles, sont générées de manière aléatoire par un algorithme.

Si vous observez attentivement, vous remarquerez des erreurs: oreilles de travers, cheveux qui ne tombent pas naturellement, arrière-plans flous, etc. This Cat Does Not Exist s'avère moins convaincant. Ces générateurs pourraient s'améliorer grâce à des données et des instructions supplémentaires. Il existe aussi un risque que de telles photos soient utilisées pour déformer la réalité, même pour de telles créations fantaisistes.

Conscients des dangers liés à l'utilisation malveillante de ce type de technologie, les chercheurs

d'OpenAI ont déclenché une tempête médiatique en annonçant qu'ils ne publieraient pas le code intégral d'une intelligence artificielle capable de rédiger automatiquement des textes convaincants à partir du contenu de 8 millions de pages web. « En raison de nos préoccupations relatives aux utilisations malveillantes de la technologie, nous avons décidé de ne pas publier le modèle dont la formation est achevée», ont-ils expliqué, qualifiant leur démarche pionnière de « divulgation responsable ».

Reconnaître les défaillances et les risques liés à une utilisation abusive de l'intelligence artificielle arrive trop rarement. Au cours des dix dernières années, les grandes entreprises technologiques qui contrôlent les médias sociaux et le commerce électronique, tant aux États-Unis qu'en Chine, ont contribué à tracer la voie à suivre pour l'intelligence artificielle. Grâce à leur capacité à recueillir d'énormes quantités de données d'entraînement, elles peuvent développer une technologie encore plus puissante. Une activité qu'elles pratiquent à un rythme effréné et qui semble incompatible avec une véritable préoccupation pour les possibles effets néfastes.

Amazon, Microsoft et d'autres se sont lancés dans la vente directe de systèmes de reconnaissance faciale aux autorités policières et d'immigration, même si, aux États-Unis, des erreurs inquiétantes et des risques graves pour les personnes de couleur ont été rigoureusement documentés et dénoncés publiquement. Les employés de grandes entreprises Internet qui développent des systèmes basés sur l'intelligence artificielle, dont Amazon et Google, ont sonné l'alarme avec insistance sur des questions d'éthique.

Les dirigeants d'entreprise font évoluer avec confiance leurs modèles économiques, vantent leur exactitude et semblent ignorer ou ne pas considérer les énormes risques liés à cette technologie. Plusieurs entreprises, dont Axxon, Salesforce et Facebook, ont cherché à apaiser les inquiétudes suscitées par les controverses en formant des comités d'éthique destinés à superviser les décisions de la société.

La cofondatrice de l'institut de recherche AI Now, Meredith Whittaker, se réfère à ces actions comme à une mise en scène de l'éthique et explique qu'aucune preuve n'indique que les décisions relatives aux produits soient réellement soumises aux comités ou qu'ils aient un vrai droit de veto. Dans une interview pour *Recode*, Meredith Whittaker a demandé aux entreprises si elles allaient nuire à l'humanité et, plus précisément, aux populations historiquement marginalisées, ou si elles comptaient se ressaisir et apporter des changements structurels importants afin de garantir le développement de produits et de services sûrs et non préjudiciables.

Il se trouve que l'annonce de Google au sujet de la création d'un comité d'éthique s'est retournée de manière spectaculaire contre le groupe qui a dissout l'organe en avril 2019 après les protestations des employés et l'indignation publique concernant les personnes invitées ou pas à y prendre part. Bien que l'entreprise se soit exprimée haut et fort au sujet de l'établissement de principes à suivre pour développer des intelligences artificielles et engagée dans des projets d'intérêt social, elle définit des priorités contradictoires à travers ses nombreuses activités.

Quels dilemmes éthiques du monde physique ces comités pourraient relever s'ils suivaient les conseils de Meredith Whittaker ? Une option consisterait à s'interroger sur une fonctionnalité du quotidien qui affecte des milliards de personnes. YouTube, la plateforme vidéo détenue par Google, est souvent considéré comme un « terrier de lapin » : des tunnels sans fin qui relient les vidéos entre elles. Même si YouTube le

réfute, les études montrent que les algorithmes de recommandation de contenu alimentent la désinformation et les croyances de type sectaires, par exemple sur les vaccins, le cancer, les discriminations sexuelles, le terrorisme, les théories du complot et [ajoutez votre sujet].

De même, Pinterest et Amazon suscitent également l'intérêt des utilisateurs par l'apprentissage qu'ils offrent et la proposition de nouveaux contenus intéressants. Tous deux rencontrent des variantes du même problème. En réponse aux scandales publics, elles ont annoncé des efforts afin d'interrompre la propagation de contenus anti-vaccins, mais peu d'éléments traduisent un véritable changement dans l'intention première ou le fonctionnement de base de ces systèmes.

Mais il n'y a pas que les entreprises du secteur technologique qui doivent se questionner sur la dimension éthique de leur utilisation de l'intelligence artificielle. Tout le monde, des organismes municipaux et gouvernementaux aux banques et aux assureurs, doit y réfléchir.

Les autorités aux frontières de neuf pays de l'Union européenne ont testé un détecteur de mensonges qui repose sur une intelligence artificielle pour contrôler les voyageurs. Des systèmes qui permettent de déterminer la solvabilité de la population sont actuellement déployés sur les marchés émergents d'Afrique et d'Asie. Aux États-Unis, les assurances maladie consultent les médias sociaux et prennent en compte ces données lorsqu'elles décident qui doit avoir accès à quelle couverture de santé. L'intelligence artificielle a même été utilisée pour déterminer qui maintenir en détention.

Ces utilisations de l'intelligence artificielle sont-elles éthiques ? Respectent-elles les droits humains ? Comme chacun le sait, la Chine a commencé à évaluer les citoyens et à leur attribuer des points au moyen d'un système de crédit basé sur leur comportement social. Les autorités chinoises ciblent désormais systématiquement en Chine une minorité opprimée avec leurs systèmes de reconnaissance faciale.

Où placer la limite ?

Fondamentalement, en matière d'intelligence artificielle, deux défis distincts se posent aujourd'hui : corriger les erreurs que nous sommes conscients de commettre et déterminer comment l'intelligence artificielle peut s'avérer bénéfique.

Exclure la dimension humaine des procédures gouvernementales et opérationnelles peut rendre ces dernières plus efficaces et moins coûteuses, mais parfois nous sommes loin de sortir gagnants de l'application de tel dispositifs.

Les citoyens questionnent trop rarement la pertinence des mesures mises en place. De même pour leur efficacité. Il y a lieu de s'interroger sur l'utilisation de l'intelligence artificielle à des fins prédictives et sur son importante présence dans nos foyers.

Une partie des erreurs les plus importantes découle de données d'apprentissage erronées ou simplement utilisées sans admettre les graves biais ayant influencé leur collecte et leur analyse.

Par exemple, certains systèmes automatisés qui présélectionnent les candidats à un emploi attribuent invariablement des notes négatives aux femmes, parce que les données montrent que le domaine en question est actuellement dominé par les hommes.

« Les catégories de collecte de données s'avèrent essentielles, surtout lorsqu'il s'agit de diviser les gens par catégories », affirment les

auteurs de l'ouvrage Data Feminism, qui étudie comment les décisions fondées sur des données ne feront qu'amplifier les inégalités sans l'adoption de mesures concrètes pour atténuer les risques.

Il semble que déléguer cette responsabilité aux neuf grandes sociétés qui dominent le domaine de l'intelligence artificielle agite le spectre d'un monde de surveillance et de conformité contrôlé par les entreprises, surtout tant que la diversité de genre, ethnique et mondiale fera défaut à tous les niveaux de ces entreprises. Le fait que des ingénieurs, des éthiciens et des spécialistes des droits humains étudient ensemble comment l'intelligence artificielle devrait fonctionner augmente les chances que celle-ci offre de meilleurs résultats, pour le bien de la société.

Nous commençons à peine à élaborer des demandes claires et convaincantes au sujet de l'avenir que nous voulons.

Depuis quelques années, nous voyons s'installer un mouvement qui vise à mieux comprendre les défis liés à l'intelligence artificielle. Des spécialistes en droits numériques, des technologues, des journalistes et des chercheurs du monde entier ont, de diverses manières, exhorté les entreprises, les gouvernements, les forces armées et les services de police à reconnaître les dilemmes éthiques, les inexactitudes et les risques relatifs à cette technologie.

Tout internaute soucieux de la santé d'Internet doit améliorer sa compréhension de l'intelligence artificielle. Celle-ci est désormais intégrée à presque tous les types de produits numériques et appliquée à un nombre croissant de décisions qui affectent des citoyens aux quatre coins du monde. Pour que notre compréhension collective évolue, nous devons partager ce que nous apprenons. Dans les salles de classe, Stefania Druga ouvre la voie par son travail avec des groupes d'enfants. En Finlande, une grande initiative viset à former 1 % de la population du pays (soit 55 000 personnes) aux questions liées à l'intelligence artificielle. Et vous, que comptez-vous faire ?

Lectures complémentaires

Situating Methods in the Magic of Big Data and Artificial Intelligence, danah boyd, M.C. Elish, Communication Monographs, 2017

AI Now 2018 Report, AI Now Institute, décembre 2018

Data Feminism, Catherine D'Ignazio, Lauren Klein, MIT Press Open, janvier 2019

Anatomy of an AI system, Kate Crawford and Vladan Joler, SHARE Lab and AI Now Institute, 2018

Poursuivre l'écoute

RecodeDecode podcast: Meredith Whittaker and Kate Crawford: How AI could change your life, avril 2019

Vie privée et sécurité Enjeux

Réinventer la publicité numérique

En 2018, alors que des dizaines de personnes sont tombées gravement malades après avoir mangé de la laitue romaine, les autorités de santé publique des États-Unis et du Canada n'ont pas pu déterminer où avaient été cultivées les feuilles de salades contaminées par la bactérie E. coli.

La traçabilité s'avérait impossible car le produit était passé par un trop grand nombre de mains entre le lavage, le découpage, l'emballage et la mise en rayon. La seule solution consistait à déclarer temporairement *toutes* les laitues romaines, quelle qu'en soit la provenance, impropres à la consommation.

En 2018, alors que des dizaines de personnes sont tombées gravement malades après avoir mangé de la laitue romaine, les autorités de santé publique des États-Unis et du Canada n'ont pas pu déterminer où avaient été cultivées les feuilles de salades contaminées par la bactérie E. coli. La traçabilité s'avérait impossible car le produit était passé par un trop grand nombre de mains entre le lavage, le découpage, l'emballage et la mise en rayon. La seule solution consistait à déclarer temporairement toutes les laitues romaines, quelle qu'en soit la provenance, impropres à la consommation.

Cela demande une dose d'imagination, mais comparons cette situation à ce que propose la publicité numérique « personnalisée » ou « ciblée ».

Nous n'avons aucune idée des ingrédients qui entrent dans la composition du pain quotidien d'Internet. Les publicités affichées dans nos applications mobiles et sur le Web s'apparentent à des feuilles de laitue éparpillées aux quatre coins du monde. Elles peuvent être saines, mais les informations relatives à la chaîne d'approvisionnement restent confuses et nous ne disposons d'aucun moyen de comprendre ce qui se passe.

Presque toute activité ou tout comportement généré par nos interactions en ligne peut être surveillé par une personne, un produit ou un service, à notre insu. Cela est valable pour les sites web que nous consultons, nos applications mobiles, le contenu que nous rédigeons dans nos courriers électroniques ou les indications que nous donnons aux assistants vocaux. Nous ne disposons d'aucun moyen de savoir comment différentes entreprises peuvent combiner cette salade mêlée de données avec des informations en mesure de nous identifier personnellement.

Apparemment, collecter des données sur tout ce que nous faisons présente toujours un intérêt commercial pour *quelqu'un*, qu'il s'agisse des développeurs d'applications, des assureurs, des courtiers en données, des pirates ou des escrocs. La frontière entre informations publiques et informations privées s'est fortement estompée. Votre carte de crédit est en mesure de transmettre à Google une liste des achats que vous effectuez en magasin. Votre profil destiné à faire des rencontres en ligne a peut-être été copié et revendu. Une question se pose : pourquoi ?

Toutes les données à votre sujet ne servent pas à vendre des publicités. Cependant, si les données constituent désormais une marchandise si prisée, c'est effectivement parce que le modèle économique d'Internet repose principalement sur la publicité. Voilà pourquoi nous parlons aujourd'hui d'économie de la surveillance et d'économie de l'attention. L'expression « Vous êtes le produit » précède Internet. Toutefois, elle a gagné une nouvelle popularité pour expliquer la « gratuité » de tant de contenus et services en ligne. Offrir ses données personnelles peut sembler peu cher payer. Cependant, le prix social induit menace toujours plus la liberté et les droits humains.

Concentrons-nous sur les aspects positifs : la publicité numérique a représenté une aubaine pour l'économie mondiale. Les services en ligne

gratuits ont favorisé l'essor de l'Internet mobile dans le monde entier. Les publicités ont aidé les éditeurs et les start-up à monétiser leur contenu et leurs services en ligne.

Pour certaines des entreprises les plus puissantes d'Internet, dont Google, Facebook et Baidu, les publicités constituent une source de revenus principale, même si ces sociétés ont étendu leurs activités dans de multiples directions et sur différentes zones géographiques. Pour Google et Facebook en particulier, l'accès aux données représente une source de pouvoir sur le marché mondial et un levier dans les négociations commerciales. Pour la première fois, aux États-Unis, les dépenses publicitaires numériques ont dépassé celles diffusées sur supports imprimés et à la télévision.

L'industrie de la publicité est vaste, mais selon certaines estimations, en 2018, Facebook et Google contrôlaient à eux seuls environ 84 % du marché mondial de la publicité numérique hors de la Chine. Pour réussir, ils ont conçu des produits axés sur la capture de l'attention de l'utilisateur et la maximisation de l'interaction pour générer des revenus publicitaires.

La plupart des publicités ciblées font la promotion de produits et services courants, mais ces mêmes outils peuvent tout aussi bien être exploités par des personnes aux intentions criminelles ou haineuses. En quelques minutes, vous pouvez placer des contenus sur des vidéos YouTube, dans des flux d'actualités de Twitter et Facebook et des résultats de recherche de Google. La possibilité de sélectionner le segment démographique à cibler nous a permis de constater que des annonceurs de certaines plateformes excluaient les individus d'une origine ou d'un sexe spécifique des annonces de logement ou d'emploi. Sur Facebook, certains vont jusqu'à cibler des « groupes d'affinité », comme les « personnes qui détestent les Juifs » (véridique…). Facebook a indiqué que ses catégories provenaient d'algorithmes et, face aux questions à ce sujet, que les catégories connaîtraient des modifications. Cependant, de telles situations soulèvent la question de la quantité de données collectées et à quelles fins.

Votre profil de données se compose des informations que vous partagez sciemment ou non. Il est interprété par des algorithmes secrets qui utilisent des corrélations statistiques. Par exemple, une recherche en ligne pour les termes de « remboursement de prêt » donne de possibles indications sur vos finances. Les mentions « J'aime » distribuées à des articles et les groupes que vous rejoignez sur Facebook constituent autant de renseignements sur vos affinités.

« La publicité peut respecter davantage la vie privée. Mais les sociétés cotées en bourse ont le devoir de maximiser les profits de leurs actionnaires, ce qui signifie pour certaines d'entre elles, d'extraire chaque goutte de données de leurs utilisateurs », explique Casey Oppenheim, PDG de Disconnect, un outil de protection de la vie privée qui bloque les traqueurs et préserve les informations personnelles des technologies indiscrètes.

La comparaison avec une crise de santé publique (telle que celle de la laitue) s'explique en grande partie par le fait que l'industrie des technologies publicitaires, bien qu'elle ait mis l'accent sur de « meilleures publicités », a négligé la protection de la vie privée pendant des années et est toujours accusée de ne pas tenir compte de la protection de la vie privée et du consentement. Même la précision relative à la valeur d'un achat publicitaire en fonction de ses vues représente un mythe. C'est un secret de polichinelle qu'une grande partie du trafic Internet dirigé vers les publicités provient en fait de robots et non d'internautes. On estime qu'en 2017 les annonceurs ont perdu près de

6,5 milliards de dollars en raison des sites web qui tirent profit de l'utilisation des robots pour gonfler leurs chiffres.

De nombreux annonceurs ont exprimé leur colère et exigé davantage de transparence dans la gestion logistique. « La Silicon Valley a instauré un fétichisme autour de l'automatisation », déclare Rory Sutherland. Le vice-président de l'agence de publicité Ogilvy au Royaume-Uni affirme que l'obsession de mesurer les résultats du ciblage a entraîné une baisse de la qualité des annonces par rapport au marketing traditionnel des médias de masse. « L'obsession du ciblage signifie que la caractéristique récompensée est la facilité avec laquelle votre algorithme identifie un client », explique-t-il. Il compare cela à une personne qui entre dans un bar avec une pancarte « Bois de la bière ! ». La plupart des gens présents sont là avec cette intention, précise-t-il. « Et les gens qui se trouvent dehors ? »

En 2017, un certain nombre d'importants spécialistes en marketing ont cessé de placer des publicités sur YouTube après une série de scandales liés à des publicités associées à des vidéos violentes et au contenu inapproprié. À l'échelle mondiale, pour le grand public, voir de tels contenus monétisés peut s'avérer dérangeant. Ce type de malaise s'ajoute à l'inconfort sournois qui augmente chez de nombreux internautes à chaque signalement d'atteinte à la sécurité des données, de failles de sécurité et de trop vastes accords de partage de données entre entreprises. Pouvons-nous réellement confier sans crainte nos données à ces entreprises?

En tant qu'internautes, nous sommes possiblement davantage « sensibilisés » à la protection de la vie privée, mais ne savons toujours pas clairement comment agir. Cependant, nous ne pouvons que souhaiter que les entreprises dont nous dépendons fortement nous protègent.

Dans un restaurant, un inspecteur de la sécurité alimentaire possède une liste des éléments à vérifier, susceptibles de représenter un danger pour la santé publique. L'Index de responsabilité des entreprises établi par Ranking Digital Rights constitue une sorte de liste de contrôle complexe qui classe ce que les plus grandes entreprises d'Internet et de télécommunications révèlent sur leurs agissement en matière de protection de protection de la vie privée et de la liberté d'expression des utilisateurs. En notant publiquement les entreprises, dont aucune n'obtient un score élevé, l'organisation, petite, mais influente, incite les entreprises à s'améliorer d'année en année et institue une méthode pour suivre les progrès et les reculs notables au fil du temps.

Nathalie Maréchal, analyste de recherche principale chez Ranking Digital Rights, à Washington, dirige un processus de consultation ouvert qui vise à créer des indicateurs entièrement nouveaux pour l'index au sujet de la publicité ciblée. « Nous devons décider ensemble des normes de divulgation et des bonnes pratiques à mettre en œuvre pour obliger ces entreprises à rendre des comptes », déclare-t-elle. Les idées actuelles en matière de meilleures pratiques de Ranking Digital Rights ne surprendront pas de nombreux chercheurs et organisations de défense d'Internet et des droits numériques. Elles suggèrent, entre autres, que les entreprises autorisent la surveillance par une tierce partie des paramètres relatifs aux publicités (par exemple, les « affinités ») et de leur financement. Elle indiquent aussi que les entreprises devraient énoncer des règles concernant les contenus interdits et l'utilisation des robots, et publier régulièrement des données pour montrer comment ces règles sont appliquées.

De tels outils et pratiques ont déjà commencé à voir le jour dans les entreprises, pas de leur propre initiative, mais sous l'effet de la

réglementation ou de la pression publique. Facebook a annoncé que la plateforme déploiera des outils pour favoriser la transparence relative aux publicités politiques à l'échelle mondiale d'ici juin. Google indique qu'en 2018 l'entreprise a éliminé plus de deux milliards de « mauvaises publicités ». De son côté, Facebook a pris des mesures pour supprimer 5000 catégories publicitaires afin de prévenir la discrimination. Depuis 2017, Twitter recueille davantage de données personnelles, mais offre désormais aussi la possibilité de modifier la manière dont la plateforme vous étiquette.

Les réglementations relatives à la protection des données s'améliorent dans de nombreux pays. De plus, les tribunaux et la société civile interpellent les entreprises du monde entier sur leurs pratiques en matière de collecte de données et de consentement au sujet de la publicité ciblée. Les réglementations s'avèrent utiles, tout comme la technologie. Dans le but de préserver les utilisateurs, la plupart des principaux navigateurs ont introduit différents types de mesures de protection contre le pistage (et parfois également des bloqueurs de publicités). Le blocage total ou partiel des publicités par différentes entreprises et selon diverses configurations est devenu une pratique courante pour des centaines de millions d'internautes. Il rend le Web plus rapide et économise nos batteries.

Revenons à nos salades. Si nous prenons l'exemple de l'approvisionnement direct chez le producteur local, prôné par l'activisme alimentaire, comment le transposer à la publicité numérique ? Peut-être pourrions-nous voir qui finance les annonces, comprendre pourquoi nous sommes ciblés et contrôler qui collecte nos données et à quelles fins.

La réflexion qui doit évoluer aujourd'hui est liée à l'idée que les publicités numériques ne sont efficaces que lorsqu'elles sont ciblées et que les entreprises savent tout sur tout le monde. Nombre de marques et de spécialistes en marketing se détournent de cette vision, par manque de preuves. À moins que les sociétés Internet puissent regagner notre confiance en modifiant leurs pratiques (ou par l'obligation du secret professionnel , à l'instar des médecins et des avocats), nous pouvons nourrir un certain espoir grâce à une nouvelle génération d'initiatives logicielles, qui explorent des solutions décentralisées pour donner aux utilisateurs un contrôle personnel afin de savoir qui a accès à leurs données.

« J'ai travaillé 10 ans pour une organisation de santé environnementale. J'y ai toujours vu des parallèles avec le monde de la protection de la vie privée, déclare Casey Oppenheim. « Tout comme nous pouvons promouvoir parmi la population des valeurs autour de l'alimentation, nous pouvons promouvoir des valeurs au sujet de leurs données. »

Lectures complémentaires

A Grand Bargain to Make Tech Companies Trustworthy, Jack M. Balkin, Jonathan Zittrain, The Atlantic, 2016

It's time for a Bill of Data Rights, Martin Tisne, MIT Technology Review, 2018

Corporate Accountability Index, Ranking Digital Rights

Décentralisation Enjeux

Le pouvoir des villes

Quand la liseuse Kindle d'Amazon a été commercialisée, les livres électroniques de cette entreprise n'étaient pas compatibles avec les lecteurs d'écran les plus courants, ce qui rendait l'accessibilité difficile pour la communauté malvoyante.

Aux États-Unis, la Fédération nationale des aveugles et malvoyants (NFB) a fait campagne pour résoudre cela pendant des années, en vain. Ensuite, en 2015, Amazon a obtenu un contrat de 30 millions de dollars avec le département de l'éducation de la ville de New York pour lancer une boutique de livres électroniques destinée aux enseignants de 1800 établissements scolaires. Les écoles municipales ont retardé le vote final jusqu'à ce qu'Amazon et la NFB trouvent une entente. Depuis, le Kindle possède un lecteur d'écran intégré et Amazon a amélioré l'accessibilité d'un grand nombre de ses produits.

Cet exemple illustre le potentiel énorme dont disposent les villes pour améliorer la santé de l'écosystème d'Internet. Dans ce cas, la victoire a bénéficié aux enfants et aux enseignants de New York, mais également au reste du monde. Lorsque les consommateurs rencontrent des difficultés à persuader les grandes entreprises d'agir d'une façon que celles-ci considèrent contraire à leurs intérêts commerciaux, un contrat d'un million de dollars et un engagement à servir l'intérêt public peuvent aider.

Plus de la moitié de la population mondiale vit aujourd'hui dans les zones urbaines et, d'ici 2050, ce chiffre devrait atteindre 68 %. Les villes concentrent la richesse et le pouvoir dans la plupart des pays, mais c'est également là que se déploient et se testent de nombreuses initiatives technologiques. Les initiatives que nous pouvons considérer comme des décisions locales aujourd'hui revêtiront possiblement une importance mondiale à l'avenir.

Lorsque la Commission fédérale des communications (FCC) des États-Unis a abandonné le principe de neutralité du Net en 2018, des maires se sont rassemblés afin de combiner leur pouvoir d'achat et soutenir les fournisseurs d'accès qui ont continué à la défendre.

« Rien qu'à New York, nous dépensons plus de 600 millions de dollars par année pour fournir des services Internet aux employés de la ville et offrir des services municipaux. Nous avons donc formé une coalition ad hoc, en commençant par huit villes qui se sont engagées à passer des contrats uniquement avec des fournisseurs d'accès haut débit qui respectent les principes de neutralité du Net. Aujourd'hui, cette coalition regroupe plus de 130 villes » indique Max Sevilia, directeur des affaires extérieures du bureau du directeur général de l'informatique de la mairie de New York.

Cette histoire et bien d'autres sont mises en lumière dans une publication intitulée *New York City Internet Health Report*. Sa créatrice, Meghan McDermott, a adapté le format du Bulletin de santé d'Internet dans le cadre d'un projet de bourse de Mozilla pour étudier, entre autres, comment les villes peuvent défendre les droits numériques en entretenant des relations avec les communautés du secteur de la technologie civique.

« La défense des libertés numériques s'axe sur la façon dont nous envisageons et déployons la technologie dans les villes. L'idée est de reconquérir la dignité et retrouver les objectifs de la technologie en tant que bien public. », explique Meghan McDermott, qui a travaillé de nombreuses années à l'intersection de l'éducation et des droits numériques, notamment au poste de directrice stratégique des Hive Learning Networks de Mozilla, une communauté de pairs dédiée à la maîtrise des compétences numériques.

Lorsque des villes déploient Internet et les appareils connectés pour résoudre des problèmes, elles sont généralement qualifiées de « villes intelligentes ». Il s'agit souvent de projets qui visent à améliorer l'efficacité énergétique, les transports ou un certain nombre de services

publics. Concrètement, nous pouvons citer en exemple les poubelles munies de capteurs qui indiquent aux services de collecte des déchets lorsqu'il faut les vider ou de parcomètres en mesure d'aider les automobilistes à localiser des places de stationnement libres dans les zones très fréquentées.

Ces projets enthousiasment les responsables municipaux du monde entier et le marché mondial des technologies utilisées pour rendre les villes « intelligentes », en constante croissance, pèse des centaines de milliards de dollars. Toutefois, ce secteur se caractérise par la forte influence des intérêts commerciaux et des idéologies techno-utopiques, où les taxis volants et les hélicoptères autonomes finissent par être considérés comme une solution aux embouteillages, même s'ils ne résoudront probablement rien pour la population qui dépend des transports publics.

Les critiques les plus sévères affirment que le battage médiatique autour des initiatives de « villes intelligentes » a donné lieu à des investissements massifs dans ce qui constitue essentiellement une technologie de surveillance, sous le couvert du progrès technologique. Les villes riches en ressources comme les plus pauvres ont installé des caméras, des capteurs, des microphones et passé de faramineux contrats pluriannuels avec des entreprises aux pratiques douteuses en matière de traitement des données. De cette façon, et avec peu de considération pour la confidentialité des données, Internet s'est frayé un chemin dans les villes du monde entier, pour le meilleur ou pour le pire.

Certains considèrent la situation comme une opportunité de repenser entièrement la manière dont les villes collectent des données sur les quartiers pour améliorer leurs services, alors que d'autres y voient un manque de transparence et la recette d'un désastre en matière de droits civils provoqué par les intérêts des entreprises. Là où certains voient des lampadaires LED écoénergétiques qui aident à recueillir des données sur les piétons à l'aide de caméras, d'autres voient un filet de surveillance empiéter sur la liberté dans l'espace public et mettre en danger les populations vulnérables. Certains choix, réalisés en amont, au début du projet, participeraient à minimiser les risques d'abus. Par exemple, il appartient de s'interroger pour savoir quand un capteur thermique représenterait une meilleure solution qu'une caméra pour recueillir des données sur une foule de personnes ?

Les défenseurs des droits numériques sont considérés comme des ennemis du progrès dans de telles réflexions, alors qu'ils soulignent simplement une divergence d'opinion fondamentale sur les intérêts que la technologie devrait servir, sur la façon de faire germer l'innovation sociale et sur les données qui devraient être utilisées (ou non) dans l'intérêt public.

Prenons l'exemple des capteurs électroniques dans les conteneurs de poubelles. Pour certains, ils illustrent parfaitement la manière dont la technologie peut participer à amélioration de l'efficacité du fonctionnement des villes. Pour d'autres, comme Tamas Erkelens, directeur du programme d'innovation en matière de données à la mairie d'Amsterdam, cela traduit une démarche inefficace qui caractérise de nombreuses innovations dont l'objectif consiste à rendre les villes « intelligentes ».

« Nous n'aurions pas besoin de capteurs dans toutes les poubelles si les villes disposaient des données Google Map pour visualiser l'emplacement de foules. », explique Tamas Erkelens. « Les lieux où les gens se réunissent représentent de bons indicateurs et correspondent généralement aux endroits où se trouvent le plus de déchets. Ainsi, nous pourrions utiliser des

capteurs uniquement pour entraîner les modèles, sans créer davantage de données au moyen de machines qui contiennent des batteries qu'il est nécessaire de remplacer », déclare-t-il.

Nombre d'administrations municipales et de défenseurs des données ouvertes du monde entier envient les masses de données détenues par des sociétés telles que Google, Uber, Apple et Airbnb qui pourraient les aider à comprendre des questions cruciales relatives au trafic, au logement et à l'emploi. En 2018, l'Open Data Institute du Royaume-Uni a publié un rapport qui mentionne que les entreprises de données cartographiques devraient être tenues de partager les données géospatiales avec leurs concurrents et le secteur public afin d'empêcher la formation de « monopoles de données » et de créer de meilleures perspectives d'innovation.

Certaines entreprises, dont Uber, partagent des données agrégées avec les urbanistes. De plus, les villes deviennent plus intelligentes en matière de demandes, telles que le partage de données sur l'utilisation de scooters électriques, comme condition préalable à l'octroi de contrats. Barcelone fait partie des rares villes qui fonctionnent selon le principe qui veut que toutes les données collectées dans le cadre d'une mission relevant de l'administration locale dans l'espace public doivent être disponibles sur une plateforme commune. M. Erkelens indique qu'Amsterdam utilise son budget annuel d'octroi de contrats, soit 2,1 milliards d'euros, également dans le but de promouvoir des conditions favorables au respect de la confidentialité des données. Il ajoute que Barcelone et Amsterdam expérimentent avec des partenaires de l'Union européenne pour développer de nouvelles technologies qui offrent aux citoyens un contrôle plus direct sur leurs propres données.

Lors du Smart Cities Expo World Congress à Barcelone en novembre 2018, les directeurs généraux de la technologie d'Amsterdam, de Barcelone et de New York ont lancé ensemble la Cities Coalition for Digital Rights en partenariat avec ONU-Habitat, un programme des Nations Unies pour soutenir le développement urbain. Les villes qui se joignent à la coalition s'entendent sur une charte de cinq principes, centrés sur le respect de la vie privée et des droits humains relatifs à l'utilisation de l'Internet. Ils se sont engagés à ce que 100 villes y adhèrent en 100 jours (avant le mois de juillet prochain) et 35 villes l'ont déjà fait. Les déclarations ne s'inscrivent pas dans le marbre, mais ces villes visent à semer les graines d'un mouvement au sein duquel les municipalités revendiqueront haut et fort les droits numériques. Grâce à la collaboration et à l'établissement de pratiques exemplaires, elles tenteront de remporter la course contre le progrès technologique qui ne s'axe pas sur les principes de dignité humaine et d'inclusion.

Malgré les ambitieuses prises de position adoptées à New York, à Barcelone et à Amsterdam, les employés qui luttent pour les droits numériques à l'échelle des municipalités décrivent une bataille difficile pour amorcer un changement culturel au sein de vastes institutions, parfois conservatrices, qui comprennent de multiples agences et présentent des intérêts divergents. L'élaboration de politiques et de procédures qui permettent à toutes les agences de prendre de meilleures décisions en matière de protection de la vie privée, de données et de transparence (et de donner accès à des éléments clés de leur travail) constitue une part fondamentale du défi à relever.

C'est à ce niveau que les communautés du secteur de la technologie civique ont prospéré dans d'innombrables villes. Les initiatives qui regroupent des start-up d'utilité publique, des étudiants du secteur technique, des fonctionnaires et des citoyens engagés visent à développer de

manière collaborative des solutions informatiques pour réinventer la démocratie dans le but de rendre les villes plus sensibles aux besoins de leurs résidents. Ils travaillent de l'intérieur avec des partenaires volontaires et de l'extérieur par le biais de groupes de pression, de travaux de recherches et de prototypes qui réimaginent comment des systèmes plus réactifs pourraient fonctionner.

Les villes du monde entier occupent une place privilégiée dans la prise de décisions qui affectent la santé de l'Internet pour tous. Au niveau local, aussi bien dans les communautés rurales qu'urbaines, les citoyens ont la possibilité de s'engager civiquement en faveur d'Internet, de façon plus directe qu'au niveau national. Nous devrions saisir toutes les occasions d'influencer l'utilisation de la technologie dans nos propres collectivités et encourager les élus à devenir des experts de la défense des droits numériques. Plus nous sommes engagés localement, plus les villes seront habilitées à s'opposer aux politiques d'Internet nationales ou internationales lorsque ces dernières vont à l'encontre des intérêts de la population.

Pour les villes, l'objectif consiste à adopter consciemment des outils numériques qui véhiculent les valeurs de diversité, d'inclusion et d'équité qu'elles défendent, plutôt que de suivre la dernière tendance de « ville intelligente ».

Quand il a aidé à faciliter les conversations entre Amazon et la Fédération nationale des aveugles et malvoyants au sujet des livres électroniques, à New York, Walei Sabry travaillait à l'office pour les personnes en situation de handicap de la mairie. Depuis, il est également devenu le premier coordonnateur officiel de l'accessibilité numérique pour la ville de New York. Au sujet des « villes intelligentes », il déclare que « ces initiatives peuvent s'avérer un succès ou un échec, selon les acteurs impliqués. Les personnes en situation de handicap doivent participer à toutes les étapes du processus, parce que ce qui fonctionne améliore les produits pour tous ».

Vie privée et sécurité | Introduction

Internet, un espace sûr ?

Internet constitue le lieu où nous pourrions vivre, aimer, apprendre et communiquer librement.

Pour être nous-mêmes, nous devons être en mesure de faire confiance aux systèmes qui nous protègent. Un virage décisif dans la sensibilisation du public à la protection de la vie privée et à la sécurité dans le monde numérique s'est amorcé l'année dernière. Certains se réfèrent même au « grand réveil de l'intimité ».

En 2018, le monde apprenait que la société d'analyse de données Cambridge Analytica avait recueilli des données de millions d'utilisateurs de Facebook, à leur insu, pour les utiliser à des fins politiques, notamment pour tenter d'influencer les élections au Royaume-Uni et aux États-Unis.

Cette information a rapidement suscité l'indignation générale. Elle a déclenché des campagnes qui réclamaient que Facebook déploie un mode privé par défaut ou incitaient les utilisateurs à purement et simplement supprimer leur compte de la plateforme. Près de trois quarts des Américains et Canadiens interrogés lors de sondages ont déclaré avoir renforcé sa sécurité sur Facebook ou avoir pris ses distances par rapport au site. Facebook a été auditionné part le Congrès des États-Unis et la Chambre des communes du Canada, condamné à une amende par le Royaume-Uni et poursuivi par le District de Columbia, aux États-Unis. Les actions de l'entreprise ont chuté.

Cette crise a été le symptôme d'un problème systémique, beaucoup plus vaste: le modèle économique dominant et la monnaie du monde numérique actuel repose sur la collecte et la vente de données à notre sujet.

Notre ère numérique, riche en données, présente certains avantages. Les services de musique en continu nous recommandent des morceaux en fonction de ceux que nous avons écoutés. La reconnaissance vocale lève des obstacles à l'accès à Internet. Les urbanistes ont accès à davantage de données. Pourtant, à mesure que les appareils recueillent un nombre croissant de données, dans nos rues et dans nos maisons, une question fondamentale demeure: sommes-nous trop vulnérables?

Disposons-nous d'assez d'informations pour prendre des décisions éclairées au sujet des tests ADN commerciaux? Maîtrisons-nous correctement les paramètres de sécurité des applications et des services en ligne? Nous devrions connaître les risques d'attaques de logiciels d'extorsion, l'importance des mots de passe complexes et savoir comment juger de la sécurité des appareils que nous achetons.

Nous pouvons également soutenir les produits et services respectueux de notre vie privée, tels que les navigateurs Tor et Firefox, et exiger que les autres entreprises s'améliorent en la matière.

Mais la responsabilité d'un Internet sain ne peut reposer sur les seules épaules des individus. Rien qu'en 2018, les fuites de données de Google, Facebook, Quora, Marriott et bien d'autres plateformes ont touché des millions de personnes. En Inde, une vulnérabilité d'Aadhaar, le système national d'identification biométrique, a exposé plus d'un milliard de citoyens indiens à des risques. De plus, des entreprises de télécommunications, dont Telus, AT&T et Sprint, ont été prises en flagrant délit de vente de données de géolocalisation de leurs clients. Nous avons besoin de davantage de protection face aux agissements des entreprises et des gouvernements.

Cependant, l'année dernière des avancées positives ont également été réalisées. Nous pouvons notamment citer l'entrée en vigueur du Règlement général européen sur la protection des données (RGPD) et la collaboration des organismes de défense des droits numériques pour en assurer l'application. En outre, les pressions

des consommateurs ont entraîné le retrait du marché de plusieurs jouets vulnérables au piratage.

Mark Zuckerberg a récemment déclaré qu'il s'engageait en faveur d'une « vision axée sur la protection de la vie privée pour le réseautage social ». Toutefois, Facebook fait l'objet d'une enquête pour des accords de partage de données avec des entreprises, dont Amazon, Apple, Microsoft et Sony. Regagner la confiance des internautes, non seulement pour Facebook, mais pour le Net plus généralement, nécessitera plus que des beaux discours.

À travers le monde, les demandes pour davantage de réglementation sur la protection de la vie privée se multiplient, certaines s'inspirant de l'idée que les entreprises devraient traiter nos données avec le même soin qu'une banque traite notre argent.

Le débat sur le modèle économique qui prédomine en ligne, et sur ses implications pour la vie privée et la sécurité de nos vies numériques, se poursuivra sans aucun doute dans les années à venir. Dans ce contexte, il est important de garder en tête que la situation actuelle résulte de choix humains et ne constitue pas une fatalité technologique. Nous avons construit ce monde numérique et détenons le pouvoir de le faire évoluer.

Vie privée et sécurité | Données

Logiciels d'extorsion: un marché criminel lucratif

Nous ne savons pas qui paie les rançons réclamées par les logiciels d'extorsion et qui les perçoit. Toutefois, en regardant les protocoles publics des comptes de bitcoins associés aux logiciels de rançon, ou rançongiciels, nous pouvons suivre la trace de l'argent.

Combien débourseriez-vous pour récupérer l'accès aux fichiers de votre ordinateur ? Voilà la question à laquelle les victimes de logiciels d'extorsion sont confrontées lorsqu'elles s'y attendent le moins. En effet, leur écran affiche un message qui menace de supprimer tous les fichiers de l'utilisateur à moins qu'un paiement ne soit effectué dans un délai imparti.

« J'ai d'abord paniqué. Ensuite, j'ai utilisé un autre ordinateur pour voir combien 1,71 de bitcoin valait en dollars. », explique John, un avocat de Chicago, dans sa description de l'attaque de rançongiciel qui a temporairement paralysé son cabinet juridique en 2016.

Cliquer sur un lien malveillant ou un fichier joint qui arrive par courrier électronique peut déclencher une demande de rançon sur les ordinateurs en réseau ou les téléphones portables. Ces logiciels d'extorsion peuvent provoquer l'effondrement des fournisseurs de soins de santé et menacer l'industrie de l'aviation. Le nombre de personnes et d'entreprises touchées par les rançongiciels varie selon les estimations, mais il s'agit d'une activité criminelle importante. Le logiciel derrière de telles attaques peut être facilement acheté et personnalisé. La société de sécurité des réseaux SonicWall a répertorié plus de 200 millions d'attaques dans le monde en 2018. Cisco estime qu'une entreprise est victime de ce procédé toutes les 40 secondes.

Au cours des dernières années, des cabinets internationaux d'avocats et des sociétés de sécurité ont collaboré dans le cadre de l'initiative No More Ransom pour partager librement des outils de déchiffrement. Cette aide s'est avérée utile pour des personnes dans le monde entier. La création de sauvegardes fréquentes et la mise à jour du système d'exploitation restent la meilleure solution pour garder vos appareils en bonne santé et exempts de logiciels malveillants par ailleurs susceptibles d'infecter d'autres machines.

Le secret obscurcit ce que nous savons sur l'impact économique des logiciels d'extorsion. Une étude réalisée en 2018 sur les paiements de rançons en bitcoins offre un aperçu du nombre de personnes qui subissent ces attaques et propose une nouvelle méthode de comptage pour mieux estimer les millions de dollars versés en rançons.

Lectures complémentaires

The No More Ransom Initiative

On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective; Mauro Conti, Ankit Gangwal et Sushmita Ruj, 2018

With Ransomware, It's Pay and Embolden Perpetrators, or Lose Precious Data, The New York Times, mai 2017

Une journée de paiements de rançons pour des attaques au moyen de WannaCry

Le 15 mai 2017, l'équivalent de 24 246,51 USD en paiements de rançons a été transféré aux responsables d'attaques WannaCry. Selon les estimations, en quelques jours, environ 300 000 entreprises ont été ciblées dans 150 pays. Aujourd'hui encore, WannaCry fait des victimes.

On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective de Mauro Conti, Ankit Gangwal et Sushmita Ruj. In: arXiv:1804.01341 [cs], 2018. Données fournies par Ankit Gangwal. Les valeurs de bitcoin en USD ont été calculées selon les taux du 15 mai 2017.

De l'importance de l'anonymat

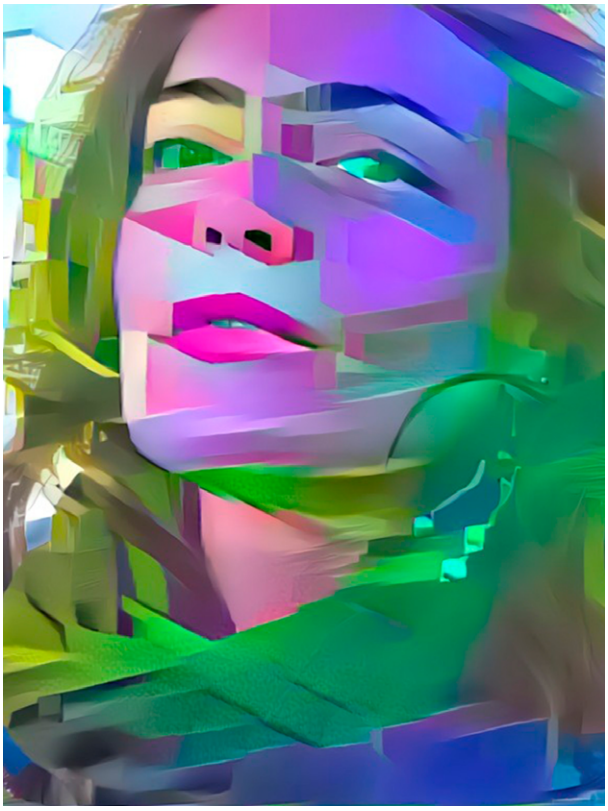
Sur Internet, lorsque des atrocités se produisent, l'anonymat est souvent montré du doigt.

Nous pourrions logiquement imaginer que la possibilité d'identifier chaque internaute permettrait de prévenir la criminalité. Dans toutes les parties du monde, des gouvernements soutiennent l'interdiction du chiffrement ou la suppression des sites anonymes. En réalité, l'anonymat protège souvent les victimes de crimes, qu'il s'agisse d'atteintes aux droits de l'homme, à la sécurité bancaire, à la défense militaire ou à la sécurité personnelle, par exemple le harcèlement et les violences familiales.

La surveillance constante, facilitée par la technologie, exercée par les entreprises ou les gouvernements, nuit à la société et aux libertés civiles. Notre capacité à communiquer, à travailler et à apprendre sur Internet, loin du regard des autres, rend de belles choses possibles.

Ne pas laisser de traces sur Internet demande des efforts. Pour ce faire, Tor constitue l'un des plus importants outils en matière d'anonymat et de contournement de la censure. Selon les estimations, il est utilisé dans le monde entier par 2 millions de personnes quotidiennement pour cacher l'origine et la destination du trafic de leurs données lorsqu'elles surfent sur le Web et communiquent.

Face aux préoccupations relatives aux activités terroristes et criminelles en ligne, Tor est souvent vilipendé. Parmi les personnes qui



Stephanie A. Whited. Photo reproduite avec autorisation.

défendent l'anonymat au quotidien, nous pouvons citer Stephanie Ann Whited, directrice de la communication du Projet Tor.

Q : Qu'est-ce qui apporte le plus de sens à votre travail ?

R : Les libertés numériques régressent dans le monde entier. Contribuer à une force au service du bien qui offre un accès privé au Web ouvert

revêt une immense importance pour moi. Des millions de personnes accordent leur confiance au navigateur Tor et au « routage en oignon » (services cachés, NdT) pour communiquer de façon privée et sécurisée au quotidien.

Certains veulent simplement, à juste titre, limiter la quantité de données que les grandes entreprises et les annonceurs peuvent recueillir à leur sujet. Pour d'autres, Tor représente un outil essentiel contre l'oppression gouvernementale.

Lors des manifestations au Soudan cette année, l'utilisation du navigateur Tor a explosé quand les médias sociaux ont été bloqués. Il connaît aussi une grande popularité en Ouganda, spécialement depuis que ce pays a introduit une taxe sur les médias sociaux.

Q : Quelles questions des journalistes vous frustrent ?

R : Celles qui reposent sur le malentendu que Tor représente le « Dark Web ».

Les services en .onion de Tor permettent de publier et de partager des informations en ligne avec un haut niveau de confidentialité et de sécurité sans que les moteurs de recherche les indexent. Impossible de les consulter dans n'importe quel navigateur. Faire l'amalgame entre cet outil et le « dark web » et imaginer que l'ensemble des publications anonymes s'accompagnent d'un danger cause du tort à une technologie sous-estimée qui sauve des vies.

Par exemple, grâce aux services onion, les femmes ont la possibilité de partager et d'accéder aux ressources de santé féminine dans des pays où celles-ci sont interdites. Cela permet aussi aux militants de s'organiser en s'inquiétant moins d'être surveillés, dans des environnements où leurs activités peuvent représenter des enjeux de vie ou de mort. Ces outils constituent aussi un moyen de communiquer en toute sécurité pour les lanceurs d'alerte qui dénoncent des affaires de corruption. Les services onion offrent la possibilité de créer une manière plus sécurisée d'accéder à des sites populaires tels que le New York Times, Facebook ou ProPublica. Tous possèdent des adresses en .onion.

Q : Quand vous entendez parler de crimes graves commis sur des sites onion (sur le Dark Net), doutez-vous du sens de votre travail ?

R : Il est parfois contrariant d'apprendre que Tor a été utilisé à des fins criminelles, mais cela ne me fait pas douter du logiciel ou des bienfaits que seuls des outils de protection de l'anonymat comme Tor apportent. En réalité, des activités criminelles existent sur toutes sortes de sites, qu'ils aient été configurés à l'aide de services onion ou non. Se débarrasser de Tor, ou même d'Internet, ne ferait pas disparaître le crime.

Q : La couverture médiatique de Tor a-t-elle changé au fil du temps ?

R : Oui, je pense que cela provient de l'amélioration de la cohérence et de la fréquence de nos communications ainsi que de la nouvelle convivialité de Tor. De plus, un nombre croissant d'internautes commencent à réaliser dans quelle mesure les géants de la technologie exploitent leurs activités quotidiennes en ligne. Même si aujourd'hui d'autres navigateurs offrent davantage de protections en matière de confidentialité qu'auparavant, aucun n'égale l'ensemble des atouts de Tor. La presse commence à le souligner de plus en plus souvent sans réserve.

Q : Quelles actualités intéressantes marquent l'univers Tor ?

R : Tor est plus convivial et plus rapide que jamais. Un réseau décentralisé de plus de

7 000 serveurs gérés par des bénévoles dans le monde entier constitue l'épine dorsale du logiciel, et nous venons de dépasser les 40 Gbit/s de bande passante totale grâce à notre communauté d'opérateurs-relais bénévoles.

Grâce à la sortie de notre premier navigateur mobile officiel, Tor Browser pour Android, en 2018, nous sommes en mesure d'atteindre davantage de personnes dans les parties du monde où Tor s'avère le plus utile.

Lectures complémentaires

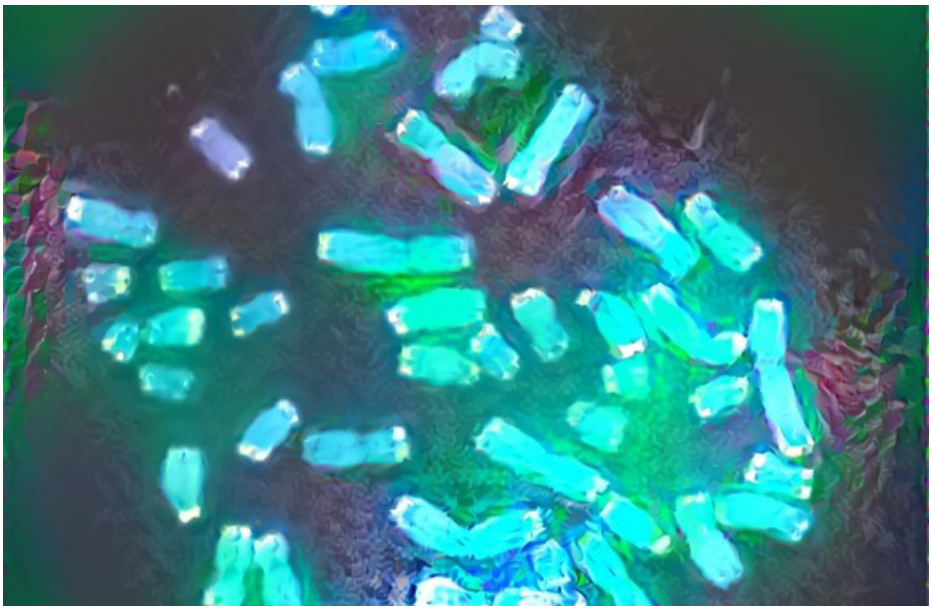
Statistiques relatives à Tor

"Tor is easier than ever. Time to give it a try", WIRED, janvier 2019

Si le problème n'est pas l'anonymat, quel est le problème ?, Bulletin de santé d'Internet, 2018

Vie privée et sécurité | Personnes

23 raisons de ne pas dévoiler votre ADN



Caryotype. Par Can H. (CC BY-NC 2.0).

Grâce à Internet, le marché des tests ADN connaît un véritable essor. Des millions de personnes ont envoyé des échantillons de leur salive à des laboratoires commerciaux dans l'espoir d'en apprendre davantage sur leur santé ou patrimoine génétique, principalement aux États-Unis et en Europe. Toutefois, certains pays interdisent de tels tests commerciaux. En France, par exemple, les contrevenants à cette interdiction s'exposent à une amende de 3 750 euros.

Les géants du secteur, Ancestry.com, 23andMe, MyHeritage et FamilyTreeDNA commercialisent leurs services en ligne, partagent les résultats des tests sur des sites web et proposent même des tutoriels sur la façon de rechercher des proches dans des annuaires ou de partager les résultats des tests sur les médias sociaux. Ils revendiquent aussi souvent des droits sur vos données génétiques et vendent l'accès à leurs bases de données à de grandes sociétés pharmaceutiques et de technologie médicale.

En ce qui concerne la santé d'Internet, nous constatons une tendance inquiétante : des entreprises acquièrent des données personnelles et agissent dans leur propre intérêt, et non dans celui du public. Bien sûr, les résultats des tests permettent parfois de faire d'importantes découvertes sur votre santé personnelle et servent à la recherche biomédicale à but non lucratif et d'intérêt public. Cependant, avant de céder à la curiosité, étudiez ces 23 raisons de ne pas dévoiler votre ADN, une pour chaque paire de chromosomes d'une cellule humaine.

1. **Les résultats peuvent être erronés.** Certains résultats en matière de santé et de nutrition personnelles ont été discrédités par des scientifiques. En 2018, l'entreprise Orig3n a identifié à tort un échantillon d'ADN d'un labrador comme étant humain. Tel qu'Arwa Mahdawi l'a écrit après avoir effectué un test ADN, « rien de ce que j'ai appris ne valait le prix et les risques d'atteinte à ma vie privée ».

2. **Les résultats relatifs au patrimoine génétique sont moins précis si vous n'avez pas de racines européennes.** L'ADN est analysé par rapport aux échantillons déjà traités. Comme les personnes d'ascendance européenne sont plus nombreuses à avoir déjà passé de tels tests, les évaluations du lieu où vos ancêtres ont vécu sont généralement moins détaillées en dehors d'Europe.

3. **Votre ADN n'offre pas d'indications sur votre culture.** Un code génétique ne renseigne pas sur tout. Comme l'écrivait Sarah Zhang en 2016, « l'ADN ne constitue pas votre culture et il n'est certainement pas garanti qu'il vous renseigne sur les lieux, l'histoire et les cultures qui vous ont façonné ».

4. **Les résultats servent d'arme aux racistes.** Les nationalistes blancs se sont massivement tournés vers les sociétés commerciales d'analyses ADN pour s'attribuer les points de « pureté raciale » les plus élevés sur les sites web extrémistes.

5. **Pas d'anonymat pour les analyses ADN.** Même si vous vous efforcez de masquer votre nom et votre localisation, votre ADN constitue un marqueur unique de votre identité, susceptible d'être utilisé à mauvais escient quoi qu'il arrive.

6. **Vous mettez en péril l'anonymat des membres de votre famille.** En confiant votre ADN à des entreprises, les personnes qui possèdent des liens de parenté avec vous (que vous les connaissiez ou non) deviennent identifiables pour d'autres, éventuellement contre leur gré.

7. **Vous vous exposez à des blessures émotionnelles.** Une telle démarche risque de vous dévoiler des éléments que vous n'étiez pas prêt à découvrir. Au Royaume-Uni, par exemple, un organisme de surveillance de la fertilité a demandé aux entreprises d'analyses ADN d'avertir les consommateurs des risques de découvrir des secrets familiaux traumatisants ou des prédispositions à développer certaines maladies.

8. **Les donneurs de sperme et d'ovules anonymes pourraient appartenir au passé.** La probabilité que les dons anonymes demeurent anonymes diminue à chaque test effectué, une réalité qui pourrait dissuader les donneurs et nuire à certaines familles.

9. **Les entreprises investissent des millions en publicités ciblées pour vous attirer.** Elles distribuent des kits gratuits lors d'événements sportifs et créent des listes de lecture spécifiques à l'ADN sur Spotify. Pour la seule année 2016, Ancestry.com a dépensé 109 millions de dollars en marketing. Une publicité

d'AncestryDNA qui capitalise sur le Brexit et la politique identitaire britannique utilisait le slogan : « Les données génétiques d'un citoyen britannique lambda sont à 60 % européennes. Nous quitterons peut-être l'Europe, mais l'Europe ne nous quittera jamais. »

10. **Une paire de chaussettes semble un cadeau plus approprié.** Vous pourriez vous laisser séduire par des offres spéciales, comme celle-ci qui offre 30 % de rabais sur les tests génétiques pour la fête des pères: « Que partages-tu avec ton papa ? Pour la fête des pères, célèbre ton lien génétique avec lui. » Pourtant, peut-être que l'homme qui possède déjà tout préfère ne pas devenir une expérience scientifique.

11. **Vous devenez un produit.** Votre code génétique est précieux. Une fois que vous décidez de partager ces informations, vous ne recevez aucune information sur les entreprises qui y accéderont ni dans quel but.

12. **Les grandes entreprises pharmaceutiques veulent votre ADN.** 23andMe a révélé avoir passé un accord de 300 millions de dollars avec le géant pharmaceutique GlaxoSmithKline en 2018 pour accéder à des données agrégées sur ses clients. Calico Life Sciences, une société de technologie médicale détenue par la société mère de Google, Alphabet, constitue le principal partenaire de recherche d'Ancestry.com.

13. **Les entreprises sont libres de modifier leur politique de confidentialité.** Dans un tel cas, peut-être que vous serez amené à donner à nouveau votre consentement, mais les politiques des entreprises sont susceptibles de changer et dans un sens qui ne vous convient pas.

14. **Une entreprise (et votre ADN) peut changer de mains.** Les entreprises sont rachetées, vendues, cessent leurs activités ou changent de modèle économique. Dans de telles situations, qu'advient-il de vos données génétiques ?

15. **Parvenir à faire détruire votre ADN peut s'avérer difficile.** Une enquête sur la façon de supprimer votre ADN d'Ancestry.com a révélé qu'il est possible d'effacer votre dossier et même de détruire l'échantillon physique de votre ADN. Mais l'entreprise ne vous facilite pas la tâche dans ce sens.

16. **Vous ne connaissez pas la durée de conservation de votre échantillon.** Certaines entreprises indiquent qu'elles conservent les échantillons pendant 1 à 10 ans. La réglementation qui régit les bases de données génétiques varie d'un pays à l'autre. Savez-vous ce qu'il en est où vous vivez?

17. **La police peut accéder à votre ADN.** Si cela offre de nouvelles possibilités en matière de résolution de crimes, l'accès à de telles informations comporte aussi des risques pour les droits humains . Les autorités ont le droit de demander aux tribunaux l'autorisation d'accéder aux bases de données génétiques des consommateurs, mais il est aussi arrivé que des enquêteurs créent de faux profils à partir de l'ADN d'un suspect.

18. **Vos résultats d'analyse pourraient figurer dans une base de données mondiale.** Dans plusieurs pays, les services de maintien de l'ordre bénéficient d'un accès illimité aux profils génétiques. Certains scientifiques soutiennent que la création d'une « base de données génétiques médicolégales universelle » représenterait le seul moyen de limiter les intrusions indésirables par la voie réglementaire.

19. **Vos données peuvent fuiter ou être piratées.** Le partage d'informations avec des tiers représente une pratique courante

parmi les entreprises. Et, plus les personnes ayant accès à votre ADN sont nombreuses, plus celui-ci devient vulnérable au piratage. Au fur et à mesure que les entreprises accumulent des données, elles gagnent en attractivité pour les criminels et le risque de faire l'objet de vols de données augmente.

20. **Il est possible de hacker des gènes.** Des scientifiques ont découvert comment stocker des données et même des GIF animés dans l'ADN. Ils pensent même que des logiciels malveillants pourraient être placés dans l'ADN pour compromettre la sécurité des ordinateurs qui contiennent ces bases de données. Alors, toujours confiance ?

21. **Vous renoncez à vos droits.** L'utilisation de services comme AncestryDNA requiert par défaut que vous autorisiez le transfert de renseignements génétiques à des tiers, libres de droits, à des fins de développement de produits, d'offres de produits personnalisées, de recherche et plus encore.

22. **Les entreprises s'enrichissent grâce à votre ADN.** Les tests proposés ne représentent pas l'unique source de revenus pour ces entreprises. Celles-ci tirent également des bénéfices des accords relatifs au partage de données passés avec des instituts de recherche et l'industrie pharmaceutique. Si votre ADN participe à développer un remède contre une maladie, vous ne le saurez jamais. Et vous ne toucherez évidemment pas un centime des ventes de médicaments liés à une telle découverte.

23. **Vous vous exposez à une future discrimination.** Aux États-Unis, les assurances de santé et les employeurs ne sont pas autorisés discriminer des candidats en fonction de leur ADN. Mais cette loi ne s'applique pas aux assurances-vie ou aux assurances-invalidité. Savez-vous quelle est la législation en la matière où vous vivez ? Quoi qu'il en soit, soyez attentif au fait qu'un jour ou l'autre, vous pourriez être obligé de partager des renseignements génétiques avec votre assurance

Si vous décidez tout de même de réaliser des tests ADN, la Commission fédérale américaine du commerce offre des conseils judicieux aux consommateurs : comparez les politiques de confidentialité avant de choisir une entreprise, choisissez soigneusement les options de votre compte, évaluez les risques et signalez tout problème aux autorités. Pour lutter contre l'emprise des entreprises commerciales, vous avez également la possibilité de vous tourner vers des bases de données de recherche à but non lucratif comme All of Us ou DNA.Land, soumis à l'examen public.

Si vous regrettez un choix passé, vous pouvez demander la suppression de vos données génétiques et la destruction de votre échantillon. Les analyses ADN illustrent parfaitement l'importance d'une législation solide en matière de protection des données. En Europe, le Règlement général sur la protection des données (RGPD) offre certaines protections, mais ailleurs, vous bénéficiez de peu de droits quant au transfert de données sensibles.

Lectures complémentaires

How DNA Testing Botched My Family's Heritage, and Probably Yours, Too, Gizmodo, 2018

Ancestry wants your spit, your DNA and your trust. Should you give them all three?, McClatchy, 2018

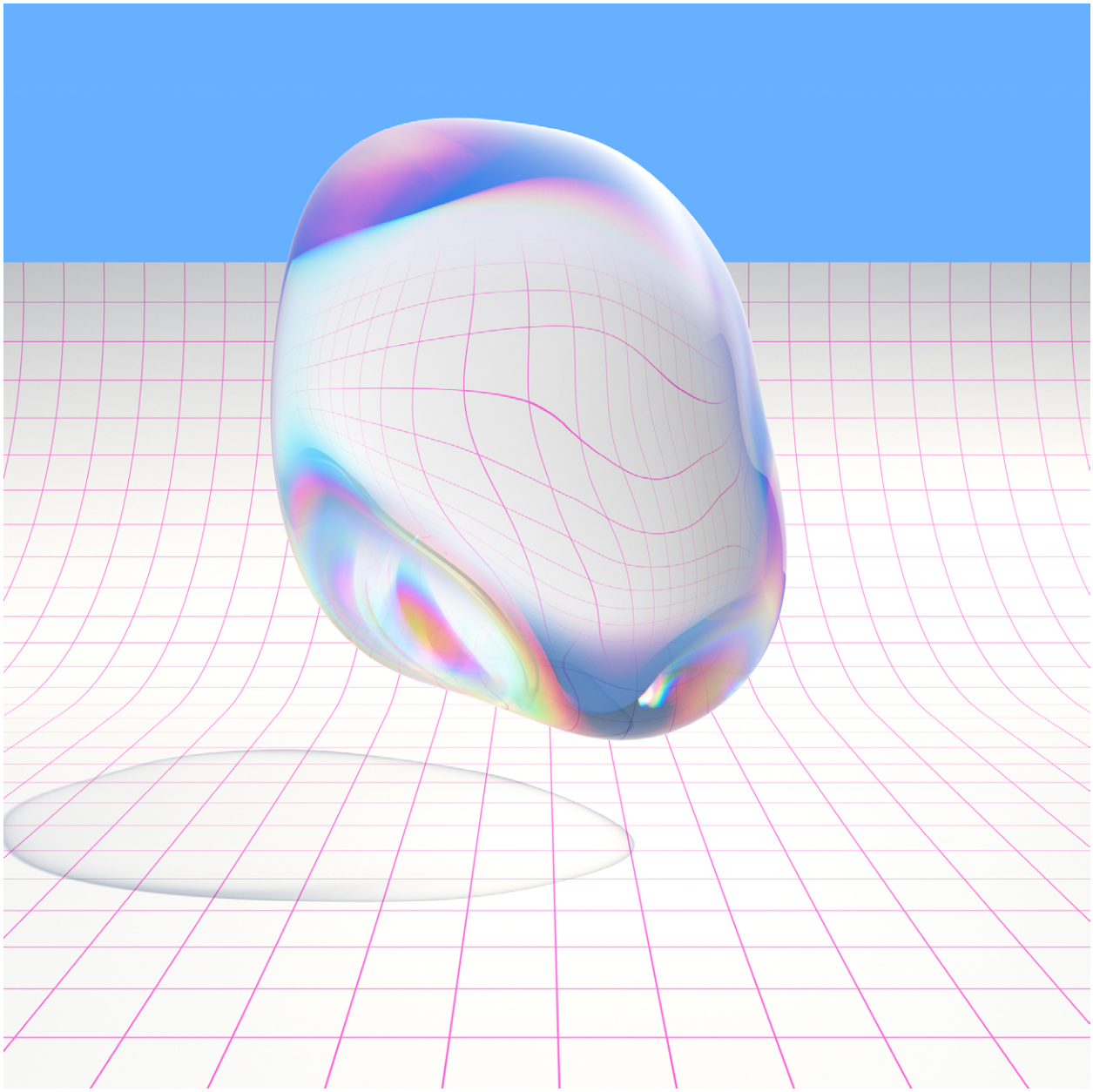
The Forensic Genetics Policy Initiative – Country Wiki

Vie privée et sécurité

Plus de contenu disponible en ligne

Coordonner les plaintes relatives à la protection des données en Europe

Vos applications mobiles vous traquent



Ouverture Introduction

Ouvert, jusqu'à quel point ?

Internet possède un pouvoir de transformation parce qu'il est ouvert : chacun peut participer et innover. Toutefois, cette ouverture n'est pas garantie, elle fait constamment l'objet d'attaques.

L'ouverture constitue un pilier fondamental d'Internet. Le monde numérique d'aujourd'hui existe parce que les individus ne nécessitent pas d'autorisation pour créer pour et sur le Web.

Pourtant, en 2019, l'ouverture d'Internet s'avère plus radicale – et plus menacée – que jamais.

Les gouvernements du monde entier continuent de restreindre l'accès à Internet de multiples façons : la censure pure et simple, obligation de payer des taxes pour utiliser les médias sociaux, blocage ou ralentissement d'Internet pour museler les voix dissidentes. De puissants lobbyistes gagnent des batailles en faveur de régimes de droit d'auteur plus restrictifs et les grandes plateformes technologiques nous enferment dans des systèmes propriétaires.

Toutefois, le Web ouvert fait preuve de résilience.

Les bénévoles de la communauté Wikidata de Wikimedia ont créé une structure de données qui permet à des individus et des machines de lire et de modifier le contenu. Les partisans des données ouvertes réclament plus de transparence pour comprendre comment les entreprises créent nos profils numériques et l'utilisation de ces données.

Une tension entre ouverture et inclusion persiste. Malgré les nombreuses mesures prises, les propos haineux et le harcèlement sur les plateformes en ligne demeurent des problèmes urgents et graves.

En Allemagne, un an après sa mise en œuvre, la nouvelle loi pour lutter contre les propos haineux ne semble ni particulièrement efficace pour résoudre les problèmes qu'elle ciblait, ni aussi restrictive que beaucoup le craignaient.

Pourtant, le manque de preuves solides n'empêche pas l'adoption de règlements semblables ailleurs. L'Union européenne débat actuellement de nouvelles règles qui obligeraient les entreprises de toutes tailles à éliminer le « contenu terroriste » dans un délai d'une heure, sous peine de sanctions sévères.

Les opposants avertissent que la loi risque de porter atteinte aux droits fondamentaux des personnes et d'étouffer la concurrence en fixant des normes que seules les plus grandes société peuvent respecter.

L'intensification des discussions sur l'intelligence artificielle et la prise de décision automatisée introduit également de nouvelles perspectives dans ce débat.

De nouveaux outils d'intelligence artificielle conviviaux ont facilité la création d'hypertrucages : des contenus qui montrent une personne exprimant des propos qu'elle n'a jamais prononcés ou effectuant des gestes qu'elle n'a jamais réalisés. Ce type d'évolution soulève une question cruciale : comment atténuer les risques de préjudices réels que pourrait causer la mauvaise utilisation d'une technologie, en particulier pour les groupes vulnérables, sans sacrifier les avantages que nous offre un Internet ouvert ?

Parfois, la meilleure approche consiste peut-être à ne jamais le diffuser.

OpenAI a récemment développé un modèle qui rédige du texte automatiquement et les résultats se sont avérés si convaincants que l'organisme s'est inquiété d'une possible utilisation malveillante. Pour éviter les risques, il a décidé de publier une version limitée du code de l'outil. Cette résolution a suscité des critiques. Certains considèrent la décision « contraire à l'ouverture »,

tandis que d'autres ont applaudi un nouveau « seuil franchi pour l'éthique ».

Relever le défi de maintenir un Internet ouvert, tout en construisant un monde numérique inclusif, reste une tâche essentielle pour les entreprises, les technologues, les décideurs politiques et les citoyens.

Et cela est d'autant plus vrai qu'une nouvelle dimension apparaît, centrée sur une question urgente : comment décider quelles technologies construire et utiliser ?

Ouverture Données

Montre-moi mes données et je te dirai qui je suis

« Arrêtez de nous manipuler et donnez-nous de véritables choix », demande Katarzyna Szymielewicz, experte en technologie et en droits humains, avocate et militante, qui lutte pour que les internautes obtiennent davantage de contrôle sur le traitement et l'utilisation de leurs données.

Les entreprises dressent nos profils numériques, constitués des données collectées par des milliers de traqueurs dans des applications mobiles ou sur le Web. Elles recueillent des informations à notre sujet pratiquement chaque fois que nous sommes connectés à Internet. Ensuite, les courtiers en données les vendent à quiconque accepte d'en payer le prix. Ainsi, ces données passent entre les mains d'innombrables entreprises à notre insu.

Les données à notre sujet sont réparties dans des catégories souvent invisibles pour les personnes concernées et analysées à l'aide d'algorithmes dont nous ne connaissons généralement pas l'existence, puis utilisées pour prendre des décisions en mesure d'avoir une incidence sur notre vie, pour le meilleur ou pour le pire.

Mais que se passerait-il si nous sortions de l'équation les hypothèses et *indiquions* simplement aux entreprises qui nous sommes ? Respecteraient-elles nos réponses ?

Katarzyna Szymielewicz a cofondé et préside la fondation Panoptykon, une organisation de défense des droits numériques en Pologne. En janvier 2019, Panoptykon a déposé une plainte contre Google en vertu du nouveau Règlement général européen sur la protection des données, alléguant que l'entreprise avait enfreint les exigences selon lesquelles l'entreprise doit fournir aux utilisateurs l'accès aux données les concernant.

Pour aider un public plus large à visualiser à quel point il nous est impossible de contrôler nos profils numériques, Katarzyna Szymielewicz utilise l'image des « trois couches » de données et fournit des exemples.

Q : Les profils élaborés à partir de nos données s'avèrent-ils inexacts ?

R : Qui sait ? En l'absence de transparence et sans accès aux profils complets générés pour nous par les sociétés technologiques, nous ne pouvons pas réellement nous prononcer. Je suis persuadée que les utilisateurs eux-mêmes

seraient les mieux placés pour contrôler ces jeux de données, puisqu'ils possèdent de réelles motivations (souvent économiques) à ne pas souhaiter être jugés sur la base d'informations incorrectes ou incomplètes. Toutefois, ils ne possèdent pas la possibilité de procéder ainsi.

J'ai imaginé cette image en plusieurs couches pour expliquer la complexité (et les dangers) du fonctionnement des profils de données en ligne après avoir entendu pour la centième fois : « Où est le problème si nous décidons de partager et de publier des données à notre sujet ? » Le fait est que ces choix ne nous appartiennent pas véritablement. Nous sommes poussés à partager plus de données que ce que nous accepterions, observés et qualifiés par des machines d'une manière difficile à imaginer. Sans surprise, celles-ci détectent des caractéristiques sensibles que nous préférerions garder privées.

Q : Pourquoi vouloir consulter nos données ?

R : La seule façon de reprendre le contrôle total de nos profils consiste à convaincre les entreprises qui réalisent le profilage de changer d'approche. Au lieu de nous cacher nos données, elles devraient faire preuve d'une plus grande transparence. Nous devons ouvrir ces systèmes opaques à l'examen des utilisateurs.

D'un autre côté, au lieu de deviner notre localisation, nos relations ou nos désirs cachés dans notre dos, les entreprises pourraient commencer à simplement nous poser des questions et respecter nos réponses. Je vois même cela comme une réelle opportunité pour les sociétés de marketing d'instaurer la confiance et de rendre les publicités ciblées plus pertinentes et plus justes.

Au sein de l'Union européenne, nous disposons d'un cadre juridique qui facilite une plus grande ouverture et un meilleur accès. Le règlement général sur la protection des données (RGPD) accorde désormais aux Européens le droit de vérifier les données détenues par des entreprises individuelles, y compris les profils marketing et publicitaires. Les entreprises restent en mesure de protéger leur code et leurs algorithmes, considérés comme des secrets d'affaires, mais en théorie, elles ne peuvent plus cacher les données personnelles qu'elles génèrent au sujet des utilisateurs. Je dis en théorie, parce qu'en pratique les entreprises ne présentent pas le tableau complet de la situation lorsqu'elles sont confrontées à cette obligation légale. Elles masquent en particulier les données d'observation des comportements et les données générées avec des algorithmes propriétaires. La situation doit changer et je suis persuadée qu'elle évoluera lorsque les premières plaintes seront déposées et donneront lieu à des amendes.

Q : Comment voir la transparence radicale devenir réalité ?

R : Nous devons nous préparer à un travail de longue haleine. Nous devons travailler ensemble en tant que mouvement et tester différentes approches. Certains d'entre nous poursuivront la voie juridique et combattront nos adversaires devant les tribunaux ou les autorités de protection des données. D'autres plaideront en faveur de meilleures protections juridiques, par exemple dans le prochain Règlement européen sur la protection de la vie privée électronique. Et, d'autres encore, développeront ou financeront en masse de nouveaux services ou pousseront les grandes entreprises technologiques à se tourner vers de nouveaux modèles économiques, et ainsi de suite. La route sera longue, mais en tant que mouvement, nous prenons au moins la bonne direction. Le principal défi pour nous aujourd'hui consiste à convaincre ou contraindre les entreprises à suivre la même voie.

Lectures complémentaires

Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy, Wolfie Christl et Sarah Spiekermann, 2016

Data Ethics – the new competitive advantage, Gry Hasselbalch et Pernille Tranberg, 2016

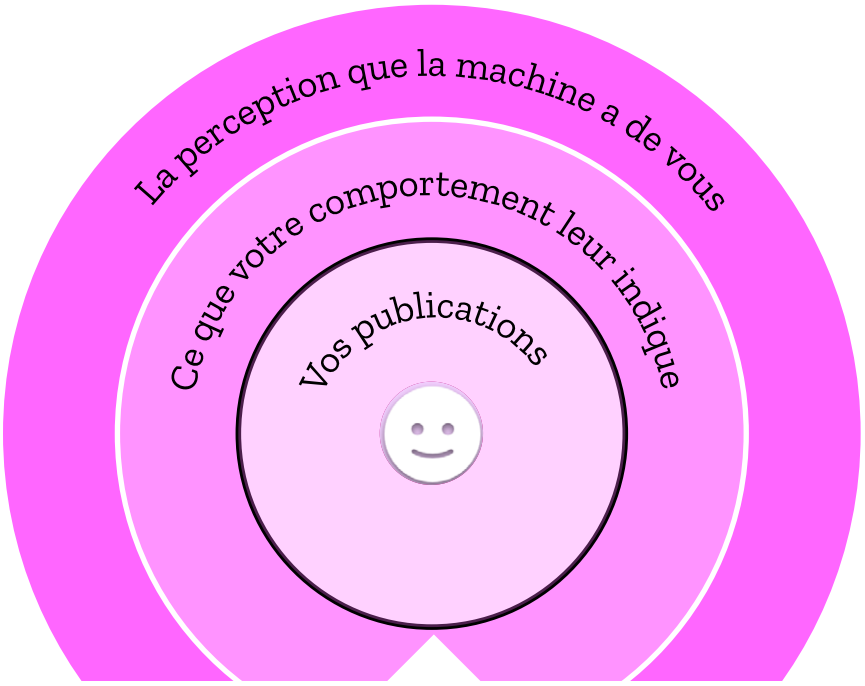
The Age of Surveillance Capitalism by Shoshana Zuboff review – we are the pawns, The Guardian, 2019

Your digital identity has three layers and you can protect only one of them, Quartz, 2019

Poursuivre l'écoute

All Your Data Are Belong to Us, IRL podcast, S.1 E.1, 2017

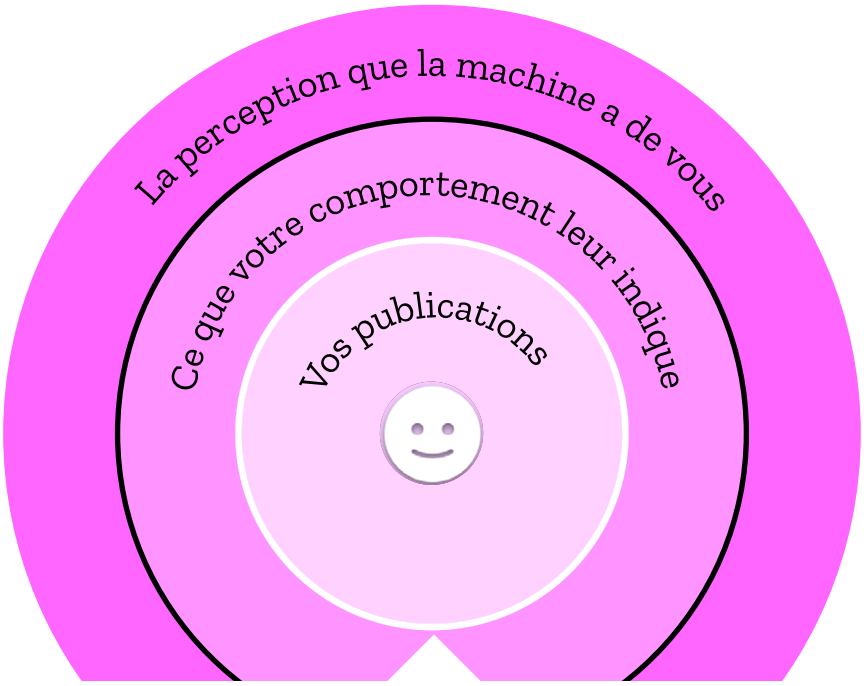
Un profil numérique à trois couches



Vos publications

La première couche représente les informations que nous proposons nous-mêmes aux réseaux sociaux et aux applications. Elles comprennent par exemple les informations de profil, les messages publics et privés, les recherches, les photos publiées ou encore les tests et sondages auxquels nous répondons.

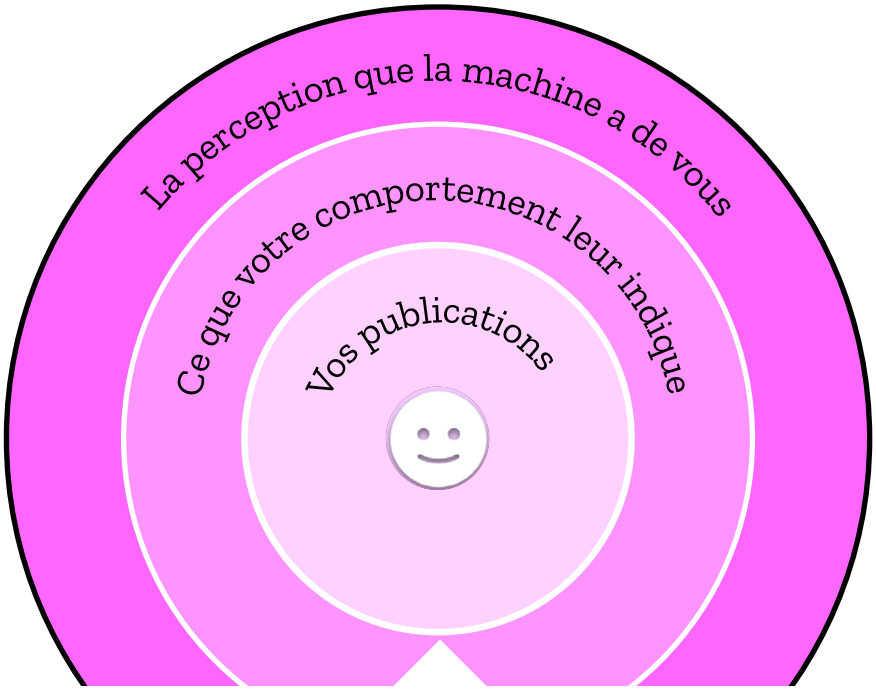
nom d'utilisateur | nom réel | genre | amis | groupes rejoints | contacts bloqués | mentions « J'aime » et autres réactions | termes de recherche | photos chargées | empreintes digitales



Ce que votre comportement leur indique

La deuxième couche comprend les données comportementales et les « métadonnées », comme notre localisation ou les personnes avec lesquelles nous communiquons dans un cadre privé ou professionnel. Il est possible de contrôler ces informations relatives à notre profil numérique, mais cela exige un effort conscient et des connaissances techniques supérieures à la moyenne.

sites web consultés
dynamique de frappe (y compris erreurs orthographiques et coquilles)
publicités cliquées
contenu ignoré
localisation de l'appareil (GPS)
articles/publications consultés
horodatage de toute activité en ligne
nombre d'interactions/publications quotidiennes
habitudes d'achat (routine)
vitesse de frappe



La perception que la machine a de vous

a troisième couche représente une interprétation automatique des deux couches précédentes. Les algorithmes nous identifient à partir de comportements et de corrélations statistiques. Ces informations sont pratiquement impossible à contrôler, car nous n'avons pas accès aux données et nous ne pouvons pas vérifier le fonctionnement des algorithmes.

affinité ethnique | grossesse | liens professionnels | opinions religieuses | affiliations politiques | profil psychométrique | niveau d'estime de soi | niveau de QI | maladie mentale | penchant pour le jeu

Three layers of our digital profile, Katarzyna Szymielewicz, Marcin Antas, Kamil Śliwowski, 2019. Les données utilisées dans cette visualisation sont basées sur les recherches de Panoptykon et se veulent des échantillons de données non exhaustifs et non applicables à chacun.

Ouverture Analyse

Les taxes sur les médias sociaux en Afrique

Photo George Pagan III sur Unsplash.

Combien paieriez-vous à votre gouvernement pour une journée d'utilisation de la messagerie WhatsApp ?

Combien paieriez-vous à votre gouvernement pour une journée d'utilisation de la messagerie WhatsApp ?

Les gouvernements de trois pays d'Afrique, l'Ouganda, la Zambie et le Bénin ont annoncé ou imposé de nouvelles taxes pour les mobinautes en 2018, laissant des millions d'Africains aux prises avec des difficultés pour couvrir leurs coûts de connexion à Internet. Au Bénin, cependant, les manifestations ont abouti à l'abandon rapide de ladite taxe.

Les gouvernements ont imposé ces prélèvements pour augmenter les recettes publiques et font également valoir qu'ils protègent ainsi le secteur local des télécommunications de la concurrence des entreprises Internet étrangères. Mais, dans la pratique, la conséquence (intentionnelle ou non) a été de retirer la possibilité de se connecter à davantage de personnes, d'accroître les obstacles à l'accès Internet et de limiter considérablement la liberté d'expression et l'accès à l'information, ainsi que l'accès aux biens et services qui se trouvent désormais en ligne.

L'Ouganda a imposé le premier de ces régimes fiscaux en juillet 2018, obligeant les résidents à payer 200 shillings (0,053 USD) par jour pour utiliser l'une des 58 applications des services de

communication mobile de tiers. Cette liste comprend notamment les réseaux sociaux tels que Facebook, Twitter, Instagram et LinkedIn, des applications de messagerie instantanée et de communication vocale comme WhatsApp, Snapchat, Skype et des sites de rencontres comme Tinder et Grindr.

En Ouganda, la loi a également imposé une taxe de 1 % sur les transactions financières mobiles, le moyen de paiement désormais requis pour recharger les cartes SIM. Alors que le citoyen ougandais moyen dépense déjà 15 % de son revenu mensuel pour 1 Go de données à large bande, la nouvelle taxe place les services Internet populaires hors de portée de la majorité de la population.

Le problème va au-delà des discussions entre amis. Comme tout le monde le sait dans la région, en Afrique, WhatsApp en particulier est devenue une plateforme essentielle pour la communication et le partage d'informations. Des millions de personnes comptent sur les groupes WhatsApp pour faire des affaires, communiquer sur les questions locales, lire les nouvelles et demander de l'aide en cas d'urgence.

Pour de nombreux Ougandais, les médias sociaux comme Facebook et WhatsApp représentent une passerelle vers le reste de l'Internet. Dans un article d'opinion pour Global Voices, la blogueuse ougandaise Pru Nyamishana écrivait :

« Cette taxe ne tient pas compte d'un manque critique d'éducation numérique, en particulier parmi la population pauvre. Lorsque j'ai interviewé des femmes à Bwaise, un bidonville de Kampala, j'ai appris que, pour elles, WhatsApp et Facebook *sont* Internet. Il s'agit des seules plateformes qu'elles savent utiliser. Aussi, avec la nouvelle taxe, elles perdront complètement leur accès à Internet. »

Après six mois d'application de la taxe, la Commission ougandaise des communications a indiqué que le taux national d'utilisation d'Internet avait chuté de 47,4 % à seulement 35 %.

Dans la foulée de l'initiative ougandaise, le Bénin a instauré une taxe similaire en septembre 2018, ciblant les services de messagerie mobile et d'appel VoIP (comme Skype). Celle-ci a fait augmenter le coût du gigaoctet de données de près de 250 %, mais a été supprimée après quelques jours de protestations publiques.

Puis, en août, le gouvernement zambien a annoncé à son tour une taxe journalière forfaitaire de 30 ngwees (0,03 USD) sur les appels VoIP. Malgré le rejet de la société civile et de la Chambre de commerce et d'industrie de Zambie, les autorités sont allées de l'avant avec cette taxe, faisant valoir qu'elle augmenterait les recettes publiques, soutiendrait les entreprises locales de télécommunications et couvrirait le coût des investissements dans les infrastructures.

« Les emplois dans les centres d'appels, les vendeurs de crédits de conversation, les techniciens d'appels traditionnels diminueront considérablement si davantage de Zambiens passent par Internet et créent des emplois aux États-Unis et ailleurs », a tweeté Dora Siliya, ministre zambienne des services d'information et de radiodiffusion.

Bien que ce raisonnement n'ait convaincu que peu d'internautes, l'argument de la ministre répond aux frustrations de longue date sur le continent au sujet des services par contournement, détenus par des entreprises étrangères qui ont conquis les marchés de la messagerie et des appels vocaux et modifié les règles du jeu pour les opérateurs nationaux de télécommunications.

Les pays d'Afrique ne sont pas les seuls à s'indigner du fait que les modèles économiques

axés sur les données et la publicité des géants du secteur technologique apportent peu de retombées bénéfiques immédiates aux économies locales, tout en enrichissant des sociétés technologiques aux États-Unis. Google et Facebook étendent toujours plus leurs activités aux infrastructures, un développement qui affectera encore davantage l'équilibre du pouvoir avec les sociétés de télécommunications. Malgré tout, il est avéré que les populaires services par contournement ont contribué à alimenter l'adoption de l'Internet mobile et permis aux entreprises locales de fonctionner plus efficacement. Cependant, ils créent aussi des dépendances en mesure d'avoir une incidence négative sur l'économie numérique locale, en particulier lorsque les priorités techniques ou commerciales changent en fonction de décisions prises loin de là.

Dans une région du monde où les gouvernements sont connus pour restreindre la liberté d'expression par la censure, les coupures d'Internet, la surveillance et les menaces juridiques, la société civile et les médias indépendants considèrent également les taxes sur ces services comme une attaque envers la liberté d'expression. Dans deux autres cas, cela est clairement mis en avant.

En avril 2018, la Tanzanie a introduit une « taxe sur les blogs », parallèlement à de nouvelles restrictions sur le contenu en ligne, dans l'intention évidente de limiter l'expression en ligne. Elle exige que les blogueurs tanzaniens, les exploitants de chaînes YouTube et les propriétaires de sites web indépendants s'enregistrent et paient environ 900 USD par année pour publier du contenu en ligne.

En août, le gouvernement mozambicain a décrété que les journalistes ainsi que les médias traditionnels ou qui utilisent des plateformes numériques doivent désormais être enregistrés et payer entre 500 et 3300 USD pour une accréditation à renouveler tous les cinq ans.

De telles taxes propagent l'idée erronée que l'accès à Internet et l'utilisation des médias sociaux constituent un luxe. Mais leurs effets, comme la baisse de l'utilisation d'Internet en Ouganda, proposent des études de cas qui prouvent l'importance de mettre en place des protections pour la neutralité du Net. Comme l'ont souligné les citoyens dans leurs contestations, et comme l'ont démontré les chercheurs, l'accès à un Internet véritablement ouvert représente une opportunité pour les économies locales, l'éducation, la santé publique et la vie en général.

Lectures complémentaires

Offline and Out of Pocket: The Impact of the Social Media Tax in Uganda on Access, Usage, Income and Productivity, Pollicy, 2019

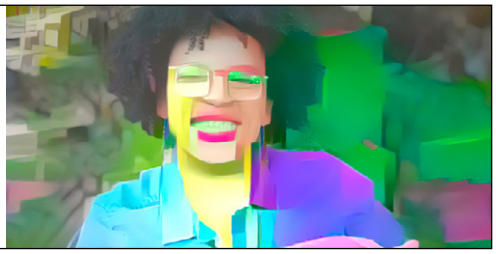
Taxed, throttled or thrown in jail: Africa's new internet paradigm, Global Voices, 2019

Eastern Africa: New tax and licensing rules for social media threaten freedom of expression ARTICLE 19, 2018

Challenges and opportunities for advancing internet access in developing countries while upholding net neutrality, Nanjira Sambuli, 2016

Plus de contenu disponible en ligne

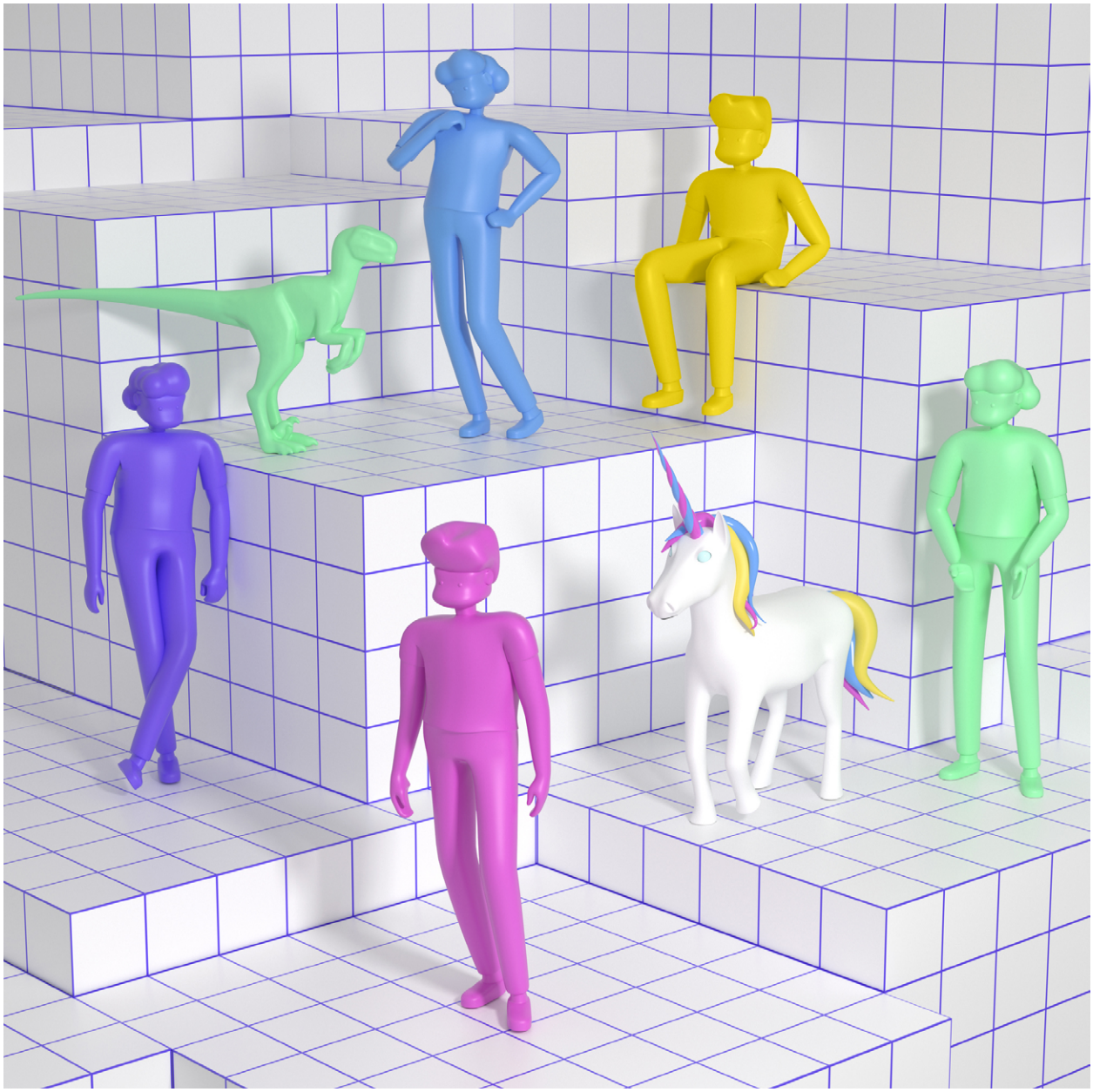
Après les coupures d'Internet, la tendance est aux ralentissements



Repérer la censure de l'information en Chine sur WeChat

Dans les coulisses de la lutte contre les contenus haineux en Allemagne

Comment réagir face aux deepfakes



Inclusion numérique | Introduction

Qui est le bienvenu en ligne?

L’inclusion numérique ne se résume pas au nombre de personnes qui ont accès à Internet. Il s’agit de savoir si celui-ci se révèle sûr et pertinent pour tous.

Une question cruciale pour la santé d'Internet demeure : comment créer un monde numérique réellement inclusif ?

Le secteur technologique lui-même se trouve aux prises avec ce défi et sa responsabilité, de plus en plus souvent dans l'espace public. De nombreuses entreprises du domaine ont fait l'objet d'accusations très médiatisées selon lesquelles leurs services facilitent la discrimination et le profilage. L'année dernière a été marquée par une vague de protestations de la part des employés des géants du secteur qui visaient, pour beaucoup, l'annulation de contrats que certains employés jugeaient contraires à l'éthique. Le personnel d'Amazon et les experts en intelligence artificielle ont demandé à l'entreprise de cesser de vendre des logiciels de reconnaissance faciale partiaux et défectueux aux autorités de maintien de l'ordre. Une lettre, signée par plus de 100 employés de Microsoft, exigeait que l'entreprise « adopte une position éthique » et annule son contrat avec les services d'immigration et des douanes des États-Unis. Jusqu'à présent, ces exigences n'ont pas été satisfaites.

Difficile d'imaginer un monde numérique vraiment inclusif alors que les entreprises responsables d'une si grande partie de son infrastructure présentent un mauvais bilan en matière d'inclusion. Nous avons assisté à certains progrès : lorsque plus de 20 000 employés de Google ont débrayé à la suite de la gestion contestée des cas d'inconduite sexuelle, certaines demandes ont été satisfaites, non seulement par Google, mais aussi par Facebook, eBay et Airbnb. Pourtant, les entreprises n'ont pas apporté l'ensemble des changements réclamés par les manifestants et beaucoup reste à faire pour que l'industrie technologique devienne un espace sûr et accueillant.

La Silicon Valley se trouve généralement au centre de l'attention du grand public, mais de nombreux torts sont à déplorer ailleurs dans le monde. Dans des usines chinoises, malaisiennes, brésiliennes et d'autres pays, des ouvriers fabriquent des téléphones portables, des montres intelligentes et du matériel dans des conditions épuisantes et souvent dangereuses, pour un maigre salaire. De grandes plateformes telles que Facebook et Twitter sous-traitent la modération de contenu à des travailleurs à bas revenus, dont beaucoup éprouvent des symptômes de traumatisme, causés par le visionnement de milliers d'images perturbantes et violentes chaque jour.

Les employés du secteur technologique qui s'organisent et défendent l'inclusion au sein de leur entreprise représentent un développement positif pour la santé d'Internet. Mais ce pas en avant semble petit devant les menaces qui pèsent sur l'inclusion numérique à plus large échelle. En effet, les auteurs de menaces et d'intimidations en ligne agissent ainsi avec la volonté de réduire au silence les femmes, les personnes non binaires et les personnes de couleur. Près de deux tiers des femmes journalistes indiquent avoir été victimes de harcèlement en ligne. Nous manquons toujours de meilleures solutions pour faire face aux discours haineux.

Toutefois, nous apprenons également de bonnes nouvelles : les codes de conduite, depuis longtemps considérés comme des outils essentiels pour l'autonomisation des personnes sous-représentées dans les logiciels libres, sont de plus en plus intégrés dans les projets à code source ouvert. En seulement cinq ans, des milliers de projets à code source ouvert ont adopté un code de conduite particulier, le Contributor Covenant.

L'accès reste également un enjeu fondamental pour l'inclusion. Le fait que plus de la moitié de la population mondiale dispose d'un accès

à Internet mérite que nous nous en réjouissions. Toutefois, en matière de connectivité, le fossé qui sépare les pays les plus riches et les plus pauvres ne s'est pas réduit au cours de la dernière décennie. La connexion la plus lente du monde s'avère aussi la plus onéreuse et les femmes sont encore beaucoup moins nombreuses que les hommes en ligne.

De toute évidence, l'égalité ne s'obtiendra pas par hasard. Le chemin vers la création d'un monde numérique accueillant pour tous reste long.

Plus de la moitié de la population mondiale dispose d'Internet, mais...

Il y a lieu de se réjouir que plus de la moitié de la population mondiale utilise désormais Internet, mais la différence des taux de connectivité entre les pays les plus riches et les plus pauvres n'a pratiquement pas diminué au cours de la dernière décennie et globalement les taux de progression ont ralenti.

Lectures complémentaires

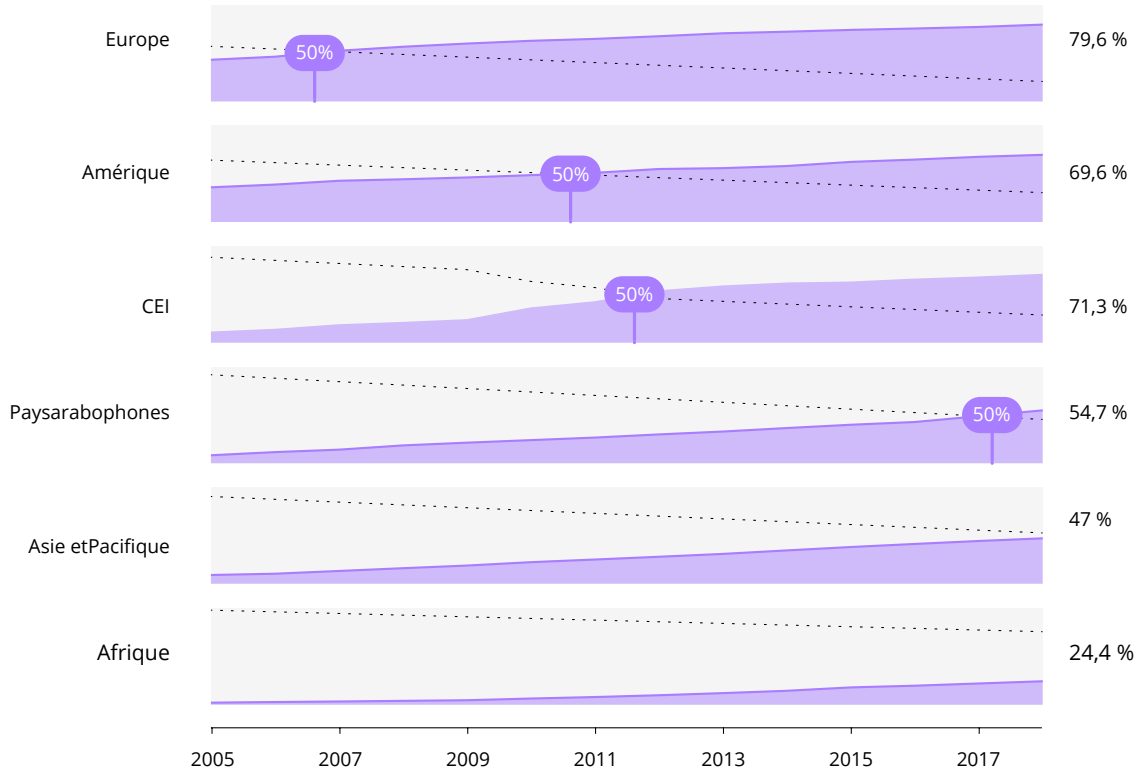
"New ITU statistics show more than half the world is now using the Internet", Union internationale des télécommunications, 2018

The Case for the Web, The World Wide Web Foundation, 2018

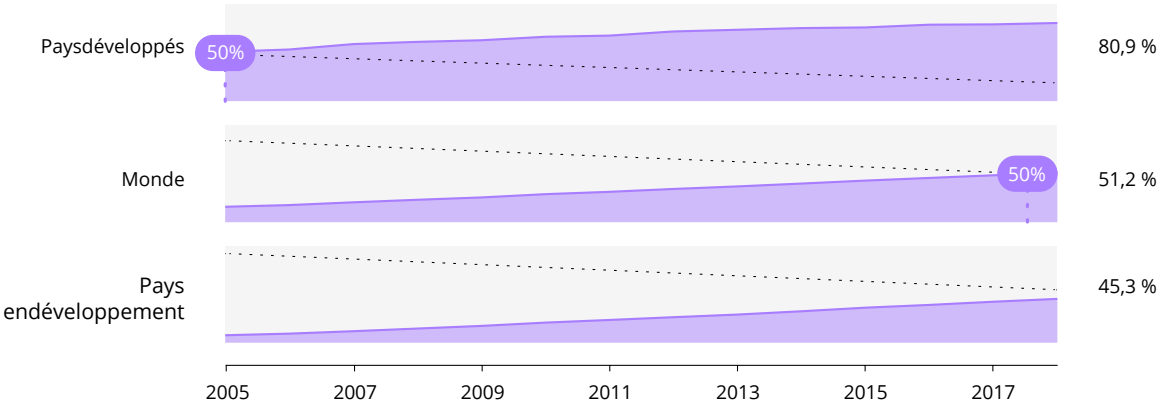
The Mobile Economy, GSMA, 2019

Accès à Internet, si la planète comptait que 100 habitants

Régions du monde



Pays développés et en voie de développement



Comment lire ce graphique

Pourcentage de personnes avec accès à Internet

Pourcentage de personnes sans accès à Internet

"Global ICT development 2001-2018", ITU statistics, 2018; 2017 Revision of World Population Prospects, United Nations DESA/Population Division, 2017

Les inégalités ne se limitent pas à l'accès. Les régions les moins connectées disposent également des connexions les moins fiables et les plus lentes aux prix les moins abordables. En outre, les femmes sont moins nombreuses à disposer d'un accès Internet, ce qui aggrave les effets des inégalités entre les sexes.

Un accès Internet pour tous et à un prix abordable constitue l'une des ambitions contenues dans les Objectifs de développement durable des Nations Unies. Il s'agit d'un prérequis pour la bonne performance d'autres facteurs de développement, notamment l'éducation, la santé et la liberté d'expression. La réduction de la fracture numérique exige une planification et des engagements à long terme de la part des gouvernements, du secteur privé et de la société civile.

Quelles régions du monde comptent plus de 50 % de personnes en ligne ?

Comment lire ce graphique

Personnes avec accès à Internet Personnes sans accès à Internet

"Global ICT development 2001-2018", ITU statistics, 2018

Des codes de conduite pour les communautés du libre

Les communautés consacrées aux logiciels libres sont animées d'une noble intention : travailler ensemble sur Internet pour concevoir des outils utiles à tous. Cependant, l'hostilité et les préjugés s'épanouissent souvent dans les communautés où les contributeurs qui adoptent des comportements non inclusifs ne sont pas sanctionnés.

Les environnements toxiques ont découragé de nombreux développeurs et développeuses de talent d'apporter des améliorations pourtant nécessaires à des projets en ligne, même aux plus importants pour le Web.

Ce facteur contribue au fait que le mouvement du logiciel libre compte seulement 3 % de contributrices, face à une majorité d'hommes blancs. Pour la santé de l'Internet, un tel manque de diversité constitue un signe inquiétant. Aujourd'hui, les logiciels libres sont omniprésents, ce qui signifie qu'un groupe très homogène de personnes contrôle des logiciels utilisés à travers le monde au quotidien.

Dans la lutte pour l'inclusion et pour des communautés plus saines, les codes de conduite se sont imposés comme l'un des outils de changement les plus importants (mais parfois controversés). Ils sont particulièrement appréciés par les groupes largement minoritaires dans cet

Coraline Ada Ehmke, 2018. (CC BY-SA 4.0)

environnement, y compris les femmes, qui les emploient comme instrument d'autonomisation pour dénoncer les comportements inadéquats.

Aujourd'hui, Apache, Google, Microsoft, Mozilla et WordPress ont tous adopté des codes de conduite pour leurs projets libres. Les communautés établies, y compris celles dont les fondateurs adoptent des manières de communiquer controversées, comme Linus Torvalds de Linux, ont été tenues, les unes après les autres, d'écouter leurs membres qui demandaient de mettre fin aux échanges grossiers et agressifs.

« Les codes de conduite sont essentiels pour les communautés du libre », explique Coraline Ada Ehmke, développeuse, défenseuse des logiciels libres et auteure du Contributor Covenant, un code de conduite adopté par des milliers de projets en cinq ans seulement.

« Un code de conduite traduit les valeurs d'une communauté », indique-t-elle.

Parmi les valeurs fondamentales figurent le soutien à un environnement ouvert et accueillant pour tous : « quel que soit l'âge, la taille, le handicap, l'identité de genre et son expression, le niveau d'expérience, l'éducation, le statut socioéconomique, la nationalité, l'apparence personnelle, l'origine ethnique, la religion ou l'identité et l'orientation sexuelles », comme mentionné dans la Charte de conduite des contributeurs.

Rien de cela ne semble pouvoir prêter à controverse. Cependant, régulièrement, des contributeurs s'inquiètent, voire se fâchent lors de l'introduction de nouvelles règles et procédures qui interdisent le langage et les comportements auxquels ils sont habitués et qu'ils ne considèrent peut-être pas blessants.

« Il existe des bonnes pratiques relatives à la rédaction de documentation ou au partage d'idées avec un groupe de personnes, possiblement inconnues, à suivre pour ne pas offenser les autres », explique Jory Burson, consultant et pédagogue qui aide les communautés du logiciel libre à bâtir une culture saine.

Emma Irwin, spécialiste des projets et des communautés du libre chez Mozilla, affirme qu'un code de conduite s'avère efficace uniquement s'il est appliqué. « La confiance vient de la mise en œuvre. La stabilité passe par la garantie de l'application. Disposer d'un code de conduite et ne pas le faire respecter peut en fait causer plus de torts » indique-t-elle.

Les limites d'une telle application sont encore en cours d'expérimentation, à mesure que les communautés cherchent comment offrir un environnement qui favorise l'égalité et la diversité. Par exemple, l'expulsion d'une communauté devrait-elle conduire à l'expulsion d'une autre?

Au départ, les codes de conduite ont été introduits à l'occasion de conférences et d'événements publics afin d'éviter les désaccords, qui allaient des questions techniques aux questions personnelles.

En 2014, après s'être engagée à ne participer qu'à des conférences qui appliquaient de telles chartes, Coraline Ada Ehmke a commencé à envisager une approche similaire pour les communautés en ligne.

« J'ai réfléchi à des moyens de faire avancer la cause de l'inclusivité au sein de la communauté technologique au sens large, se rappelle-t-elle. Ma solide expérience dans le mouvement du libre m'avait démontré que ces communautés d'éditeurs et de contributeurs nécessitaient également un contrat social pour formuler et faire respecter les valeurs communautaires en faveur d'une plus grande diversité et d'un meilleur accueil de tout type de personnes, en particulier

celles traditionnellement sous-représentées dans le secteur technologique.

Voilà comment le *Contributor Covenant* est né. »

« Au cours des sept ou huit dernières années, dans la pratique, le besoin d'un code de conduite pour les événements s'est étendu à l'espace numérique, conclut Jory Burson. C'est un très bon développement. »

Lectures complémentaires

The Woman Bringing Civility to Open Source Projects, WIRED, 2018

Open source is only ajar without inclusion, Emma Irwin, Internet Citizen (Mozilla), mars 2019

Now Intel signs up to open-source code of conduct after Torvalds' Linux hiatus, ZDNet, 2018

Your Code of Conduct, Open Source Guides, Github

L'inhumaine face cachée de la technologie

Usine d'un fournisseur d'Amazon, Foxconn Hengyang.
Crédit photo : China Labor Watch (CC BY-SA 4.0)

Dans la Silicon Valley aux États-Unis ou la Pangyo Techno Valley en Corée du Sud, travailler dans le secteur technologique s'avère souvent lucratif. Coder et concevoir de nouveaux produits peut rapporter un salaire considérable, un emploi stable et des avantages comme des repas gratuits.

Cependant, tous les travailleurs de la chaîne d'approvisionnement technologique n'ont pas autant de chance. Les travailleurs qui se consacrent à la production et fabriquent des iPhone, des montres intelligentes et d'autres matériels, dans des usines en Chine, en Malaisie, au Brésil et dans d'autres pays, connaissent parfois des conditions de travail épuisantes et inhumaines.

Li Qiang dirige China Labor Watch (CLW), une organisation basée à New York qui a pour objectif d'améliorer les conditions de travail des travailleurs chinois. L'organisation à but non lucratif mène des enquêtes qui reposent sur des opérations en infiltration dans des usines en Chine, documente les mauvaises conditions de travail et fait pression sur les entreprises pour qu'elles les améliorent. Depuis 19 ans, CLW a enquêté sur des usines qui produisent du

matériel pour Apple, Dell, Microsoft, Samsung, Huawei et d'autres grandes entreprises.

CLW a mis au jour du travail d'enfants, de affaires de discrimination, des règles qui prévoient des heures supplémentaires obligatoires et des violations des droits de l'homme. Parmi les rapports récents figurent Amazon Profits from Secretly Oppressing its Supplier's Workers (juin 2018) et A Year of Regression in Apple's Supply Chain (mai 2017).

« Ces entreprises recherchent des moyens de réduire les coûts de production, explique Li Qiang. Elles accordent peu d'attention aux conditions de travail. »

Souvent, les ouvriers en usine de Chine ne gagnent pas le minimum vital. Le salaire qu'ils touchent correspond peut-être au salaire minimum légal de la région, mais Li Qiang indique que ce n'est pas suffisant pour subvenir à leurs besoins. Par conséquent, les heures supplémentaires deviennent nécessaires et les semaines de 60 heures, ou plus, deviennent la norme.

De plus, de nombreux ouvriers ne reçoivent pas de formation adéquate en matière de sécurité. « Les travailleurs sont exposés à des produits chimiques toxiques sans même le savoir. »

Qui est responsable de ces mauvaises conditions de travail ? Li Qiang explique que les différents acteurs se renvoient la balle : « Les entreprises comme Apple et Dell considèrent que les terribles conditions de travail sont imputables aux usines. Et celles-ci rejettent la responsabilité sur les agences qui embauchent les ouvriers. »

Les terribles conditions de travail qui prévalent dans les usines chinoises ne sont un secret pour personne. En 2010, une série de suicides dans les usines de Foxconn Technology dans la municipalité de Shenzhen faisait la une de l'actualité. En 2015, WIRED publiait un article au sujet d'une adolescente de Dongguan qui travaillait 15 heures par jour dans une usine, utilisait un produit chimique toxique pour nettoyer les écrans de téléphone et constatait que ses collègues tombaient malades.

Li Qiang reconnaît que les conditions de travail se sont améliorées au cours des 20 dernières années. Il mentionne notamment le fait que les entreprises du secteur technologique s'attaquent désormais à certains problèmes : Apple publie des rapports d'évolution sur la conformité de ses fournisseurs au droit du travail et aux droits humains. Le travail de Dell en matière de responsabilité sociale comprend des initiatives qui visent à améliorer les normes de travail dans la chaîne d'approvisionnement.

Toutefois, Li Qiang souligne que les salaires restent bien trop bas. De plus, trop peu d'organisations surveillent les entreprises et militent pour des changements. Parmi les alliés de CLW figurent une centaine d'organisations membres du réseau GoodElectronics. Il s'agit d'une coalition néerlandaise à but non lucratif qui rassemble des syndicats, des chercheurs et des universitaires pour défendre les droits de l'homme et la durabilité écologique dans la chaîne d'approvisionnement électronique mondiale. Les organisations traditionnelles de défense des droits du travail, y compris l'Organisation internationale du travail des Nations Unies, étudient et offrent également des conseils sur les meilleures pratiques des entreprises.

Une bonne santé d'Internet passe par des conditions de travail humaines pour les personnes qui produisent les téléphones, les ordinateurs et autres appareils nécessaires à notre connectivité. Nous devons garder en tête que la technologie bon marché sous-entend

que certains paient un lourd tribut. Pour que le public soit rassuré sur le respect que les entreprises du secteur technologique portent à l'humanité, celles-ci doivent faire preuve de davantage de transparence et de responsabilité, et assurer une meilleure protection des droits et de la sécurité des travailleurs. Alors que notre quotidien intègre toujours plus de produits technologiques, ces questions concernent finalement chacun de nous.

Lectures complémentaires

GoodElectronics network

China Labor Watch

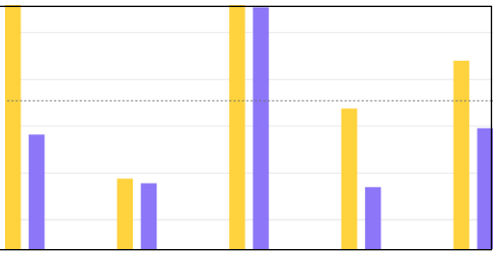
Une réponse à notre culture de la technologie jetable, Bulletin de santé d'Internet, 2018

Worker satisfaction starts with talking to factory employees, blog du fabricant Fairphone, mars 2019

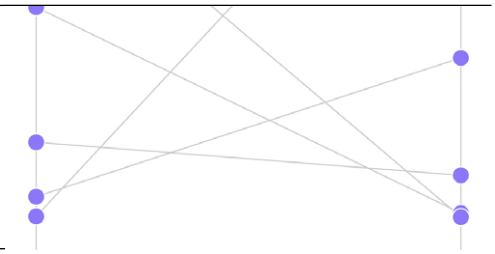
Plus de contenu disponible en ligne

Admettre le biais de l'intelligence artificielle

Les femmes journalistes plus touchées par le harcèlement en ligne



La connexion la plus lente du monde s'avère aussi la moins abordable



Les employés du secteur tech se rebiffent

La volonté mondiale d'identifier tout le monde numériquement

Éducation à Internet | Introduction

Comprendre l'enjeu

Se connecter ne représente que le premier pas, tout le monde doit acquérir des compétences pour lire, écrire et participer au monde numérique.

En 2018, le monde a franchi une étape importante: plus de 50 % de la population a désormais accès à Internet. À ce stade, les compétences web s'avèrent plus importantes que jamais.

Chaque jour, nous effectuons des centaines de choix en ligne. Pour beaucoup, utiliser notre téléphone pour acheter un café, billet de bus ou demander à un assistant vocal de lancer notre chanson préférée est entré dans les habitudes. Pourtant, pour la plupart d'entre nous, la technologie que nous utilisons au quotidien reste obscure et mystérieuse. Nous ne saisissons pas pleinement les implications de nos décisions ou de celles que d'autres prennent pour nous.

Les connaissances de base au sujet du Web s'avèrent importantes. Toutefois, elles ne nous préparent pas nécessairement à cerner et à aborder les principales questions et les défis de taille comme les préjugés, le harcèlement et la concentration du pouvoir dans notre monde connecté. Du plan personnel au plan politique, le rôle joué par la technologie dans nos vies évolue rapidement. Aussi, il est essentiel que notre compréhension du monde numérique progresse également.

Les parents partagent des photos de leur bébé sur les réseaux sociaux sans se poser de questions. Mais, à mesure que les enfants grandissent, certains considèrent que le partage en ligne d'informations à leur sujet constitue une violation de leur vie privée. Même les petites décisions ont des répercussions durables. Aussi, de solides connaissances web sont requises pour effectuer des choix éclairés.

Internet permet de rester facilement en contact avec des amis et d'entrer en contact avec des personnes qui partagent les mêmes idées. Mais, comment notre bien-être est-il affecté par le temps que nous passons à cliquer et à faire défiler notre écran ? Prendre connaissance de ce que les études indiquent (et n'indiquent pas) peut nous aider à entretenir des rapports plus sains avec la technologie.

Il est essentiel de comprendre l'incidence d'Internet sur nos sociétés et d'être disposés à exiger des changements si nécessaire. Dans la plupart des pays, Internet s'avère aussi bien bénéfique que néfaste pour les processus démocratiques. Il offre un meilleur accès aux informations sur les candidats, des données publiques plus transparentes et de nouvelles possibilités d'organisation populaire. Cependant, il facilite également l'ingérence dans le processus électoral et la diffusion de fausses informations nuisibles.

Au cours de l'année écoulée, nous avons mieux compris comment des groupes marginaux, des acteurs individuels, les gouvernements et les partis politiques exploitent les plateformes numériques pour influencer les citoyens. Lorsque les gouvernements proposent des solutions, celles-ci risquent de faire naître de nouveaux préjudices. Les « lois contre les fausses informations », adoptées dans différentes parties du monde (et dernièrement à Singapour) peuvent représenter une sérieuse menace à la liberté d'expression.

Une meilleure compréhension, plus nuancée, du monde numérique, nous offre la capacité de nous joindre aux efforts de communautés mondiales pour aider les défenseurs des droits humains à demander justice. Elle donne aussi les moyens de créer des espaces en ligne plus sûrs pour l'éducation sexuelle des jeunes et de mieux cerner les dynamiques de pouvoir en ligne, de l'économie publicitaire à la surveillance de masse.

Nous pouvons imaginer des mondes différents. Nous pouvons exiger des changements.

Il est plus urgent que jamais d'investir dans l'éducation universelle au Web. Cela passe par le soutien aux éducateurs et aux militants, ainsi que par l'apprentissage auprès de communautés inclusives. Mais, cela requiert également la conception de produits faciles à comprendre, à modifier ou à réparer.

Plus nous serons nombreux à comprendre l'évolution des technologies, des normes et des modèles économiques du monde en ligne, plus nous nous montrerons capables d'exploiter pleinement le potentiel d'un Internet sain.

Web Literacy People

L'éducation sexuelle à l'ère numérique

Si la pornographie existait bien avant Internet, chacun sait que les contenus pour adultes sont plus accessibles que jamais, y compris pour le jeune public. La façon dont les parents et les enseignants abordent ce sujet, qui représente un tabou pour beaucoup, s'avère essentielle pour adapter l'éducation sexuelle à l'ère numérique.

Les préoccupations au sujet des effets de la pornographie sur les adolescents représentent un véritable sujet de société, maintenant que 80 % des jeunes du monde entier bénéficient d'un accès à Internet.

Puisqu'une grande partie du contenu pour adultes en libre accès se caractérise par l'hypermasculinité et met en avant le plaisir masculin, la possibilité que les jeunes qui visionnent du porno puissent développer des comportements dangereux en matière de sexualité ou abusifs envers les femmes constitue une inquiétude majeure.

La plupart des recherches hésitent à établir des liens de cause à effet entre la pornographie et des attitudes ou des comportements sexuels spécifiques. Pourtant, les jeunes eux-mêmes indiquent que le visionnement d'images pornographiques, qu'ils y accèdent de manière accidentelle ou les recherchent, peut les affecter.

Emily Rothman, professeure de sciences de la santé communautaire à la Boston University

Emily Rotham, 2019. Photo Flynn Larson, par aimable autorisation de la Fondation Robert Wood Johnson

School of Public Health, étudie les liens entre la pornographie et les violences sexuelles depuis près d'une décennie. En 2016, elle a mené une étude auprès de 72 adolescents âgés de 15 à 17 ans et constaté que la pornographie représentait leur principale source d'informations au sujet de la sexualité.

Par sa démarche, Emily Rothman vise à comprendre l'importance du rôle de la pornographie chez les jeunes et à étudier comment les connaissances à ce sujet peuvent servir à réduire les risques.

Elle s'est associée au programme de soutien entre pairs Start Strong de la Commission de la santé publique de Boston pour concevoir un cours à option sur la « culture du porno » destiné aux élèves du secondaire de Boston, aux États-Unis.

Le cours, intitulé The Truth About Pornography: A Pornography-Literacy Curriculum for High School Students Designed to Reduce Sexual and Dating Violence (« La vérité sur la pornographie : un programme destiné aux élèves du secondaire, conçu pour réduire les violences sexuelles et dans les relations de couple »), offre un espace de discussion critique sur la façon dont le genre, la sexualité, le consentement, le groupe ethnique, les relations et l'image corporelle sont représentés (ou non) dans la pornographie.

Les leçons vont de la définition des termes utilisés dans la pornographie en ligne à l'aide aux élèves pour éviter de cliquer sur des contenus auxquels ils ne souhaitent pas être exposés. Les élèves sont également guidés dans des discussions délicates sur la question de savoir si la pornographie contribue aux violences perpétrées contre les femmes.

« En fait, nous voulons parler aux jeunes des relations amoureuses et des violences sexuelles », explique Emily Rothman. « Nous avons constaté qu'ils trouvent amusant de parler de pornographie. Nous abordons donc ce thème pour parler de sujets que nous estimons vraiment essentiels, comme le consentement et l'établissement de limites saines dans une relation. »

Emily Rothman considère que la meilleure façon de minimiser les effets négatifs de la pornographie chez les jeunes passe par une éducation complète, factuelle et positive en matière de sexualité. « En l'absence de toute autre forme d'éducation ou source d'informations, il y a de plus grandes chances que les jeunes se tournent vers des contenus réalisés à des fins de profit économique et de divertissement pour s'informer.

S'ils possédaient des connaissances à ce sujet avant leur premier contact avec la pornographie, ils seraient immunisés contre certaines des potentielles pires influences. »

Internet peut également jouer un rôle positif en offrant aux jeunes des espaces d'apprentissage sûrs. Par exemple, 70 % des étudiants américains LGBTQ ont déclaré avoir effectué des recherches sur leur orientation sexuelle en ligne. De nombreuses études montrent qu'Internet aide les jeunes LGBTQ à communiquer avec des pairs qui les soutiennent et ainsi possiblement renforcer leur confiance en soi.

Ce type d'incidences positives, que les défenseurs de la liberté d'expression veulent défendre contre la censure, soulignent l'importance du droit à l'anonymat. Au moins 16 pays censurent la pornographie en ligne, mais l'accès à du contenu étranger reste possible. Des groupes de défense des droits numériques, dont l'Electronic Frontier Foundation, se sont opposés aux propositions qui visent à imposer des limites d'âge pour accéder aux contenus pornographiques, arguant qu'une telle mesure

porterait atteinte à la vie privée des internautes.

En 2018, la plateforme de microblogging Tumblr a interdit les contenus pour adultes, provoquant une controverse sur la perte d'un « espace en ligne sûr » pour les communautés LGBTQ+ ainsi que les travailleuses et travailleurs du sexe. En effet, la plupart des plateformes y compris Facebook et YouTube interdisent la nudité et les contenus sexuellement explicites. Ainsi, des milliers d'internautes ne savent plus vers quelle plateforme se tourner.

Dans ce paysage numérique complexe et changeant, une affirmation reste vraie : les parents et les éducateurs peuvent jouer un rôle important d'accompagnement pour aider à sensibiliser les jeunes afin qu'ils puissent acquérir les connaissances nécessaires au développement d'une image positive de la sexualité et des relations saines. Pour les jeunes qui entreprennent leur propre voyage de découverte, Internet offre une mine de ressources (publications et communautés de soutien) à même de constituer un meilleur point de départ que le porno pour s'informer sur les questions de sexualité et de santé, notamment des sites web comme Amaze.org, Scarleteen.com et Ahwaa.org.

Lectures complémentaires

10 years on: why we still need better sex education for the digital world, Jessica Ringrose, Amelia Jenkinson, Sophie Whitehead, IOE London Blog, UCL Institute of Education, 2019

What Teenagers Are Learning From Online Porn, New York Times, 2018

Porn and sex education, porn as sex education, Kath Albury, UNSW Sydney, 2014

Adolescent Pornography Use and Dating Violence among a Sample of Primarily Black and Hispanic, Urban-Residing, Underage Youth, Emily Rothman and Avanti Adhia, Behavioral Sciences, 2016

La démocratie à l'ère numérique

Internet, un soutien ou un obstacle aux processus démocratiques dans le monde ? Dans la plupart des pays, nous constatons des effets aussi bien bénéfiques que néfastes.

À l'âge d'or d'Internet, le réseau était célébré parce qu'il offrait aux électeurs un nouvel accès à des informations sur les candidats aux élections et des niveaux inégalés de transparence en matière de données publiques. Il a jeté les bases d'une nouvelle ère de campagnes politiques et de mouvements sociaux, en proposant aux citoyens de remettre en question les structures du pouvoir en place et les détenteurs de l'information.

Aujourd'hui, cet optimisme est nuancé par les constantes affaires d'interférences dans les élections qui se sont produites sur Internet, aux États-Unis et dans de nombreux autres pays. Ces affaires ont suscité un nouveau niveau d'inquiétude parmi les institutions démocratiques. Les faits survenus dans le cadre de l'élection présidentielle de 2016 aux États-Unis ont peut-être surpris de nombreux citoyens dans le pays, mais sur la scène mondiale, il ne s'agit pas d'un événement isolé.

Prenons le Brésil. Dix jours seulement avant l'élection de Jair Bolsonaro à la présidence, le principal quotidien, *Folha de São Paulo*, a révélé une campagne de 3 millions de dollars, financé par des entreprises de l'entourage du candidat, pour diffuser des messages viraux et clivants ainsi que de fausses informations en faveur du candidat, malgré les efforts de vérification déployés par différents groupes et par Facebook pour contenir la vague de désinformation.

Peu après, la journaliste derrière cette révélation a commencé à recevoir des menaces et son compte WhatsApp personnel a été piraté et inondé de messages pro-Bolsonaro.

Les efforts visant à promouvoir les candidats par des méthodes fallacieuses et à étouffer l'information indépendante sont également très répandus en Inde. Les groupes de la société civile observent depuis longtemps sur Facebook et WhatsApp des campagnes de provocation et de désinformation qui semblent destinées à étouffer les voix dissidentes et à promouvoir le Parti Bharatiya Janata (BJP) de l'actuel Premier ministre Narendra Modi.

En prévision des élections d'avril 2019, des plateformes de médias sociaux comme Facebook et Twitter ont annoncé qu'elles avaient supprimé des centaines de pages (qui comptaient, au total, des millions d'abonnés) pour « comportement trompeur coordonné » et « promotion d'envois non désirés ». Certaines soutenaient le BJP, d'autres le Parti du Congrès national indien.

Le rôle de Facebook en particulier, dans ces élections et dans d'autres, a entraîné un important examen public. En 2018, l'audition de Mark Zuckerberg par le Congrès des États-Unis à la suite d'un scandale public impliquant le cabinet de consultants Cambridge Analytica, a joué un rôle important dans la mise en lumière de la collecte de données à des fins politiques.

Marc Zuckerberg s'était alors excusé de ne pas avoir pris davantage de mesures pour empêcher que la plateforme serve des fins préjudiciables, notamment « la diffusion de fausses informations, l'ingérence étrangère dans des élections et les propos haineux ».

Depuis, Facebook s'est engagé à renforcer la transparence en matière de publicité politique. Twitter a ajouté « l'intégrité des élections » à ses valeurs publiques. Mais de telles mesures ne constituent probablement que des solutions de fortune. En effet, les plateformes sont conçues de manière à encourager et à récompenser les contenus immodérés et sensationnalistes qui génèrent des clics et des partages, au moyen de déclarations et d'attaques scandaleuses. Les algorithmes des flux d'informations sont facilement piégés par des robots et des trolls professionnels. De même, les résultats de recherche de Google peuvent être manipulés.

En 2017 et 2018, Cambridge Analytica a également recueilli des données auprès d'utilisateurs en Inde, au Brésil, en Indonésie et au Mexique pour des missions sur des campagnes électorales. La société de conseil s'est également implantée au Kenya. Dans une étude de cas tirée de la campagne électorale de 2013 de l'actuel président Uhuru Kenyatta, Cambridge Analytica décrivait avoir élaboré une stratégie pour le candidat « basée sur les besoins (emplois) et les peurs (violence tribale) des électeurs ». Cette démarche a touché une corde sensible parmi la population kényane habituée à la violence provoquée par les médias sociaux entre les différents groupes ethniques.

En 2017, les partis kenyans ont employé la publicité ciblée et même l'envoi de messages SMS personnels destinés aux citoyens en mettant à profit l'important jeu de données personnelles collectées par le gouvernement, pour lesquelles il n'existe actuellement aucune protection juridique qui assure leur confidentialité. Le président Uhuru Kenyatta a remporté cette élection lors d'un deuxième scrutin, après que la Cour suprême eut annulé sa première victoire en raison d'irrégularités.

Ces affaires ne représentent qu'une poignée de celles qui ont fait les gros titres des journaux et des fils d'actualité dans le monde entier au cours des dernières années. Elles indiquent, en résumé, que sur Internet, toute personne qui possède les moyens financiers nécessaires et est disposée à utiliser l'information et les données comme arme peut atteindre des millions de personnes et influer sur leur opinion. Des personnes et des institutions puissantes et riches, des gouvernements locaux et étrangers, utilisent ainsi Internet à des fins politiques.

Des idées pour atténuer les risques ont commencé à émerger. Le soutien aux initiatives indépendantes de vérification des faits augmente dans le monde entier et les électeurs sont de plus en plus sensibles aux machinations numériques des dirigeants politiques et des groupes d'intérêt. Dans la perspective des élections européennes de 2019, quatre géants du secteur technologique (Facebook, Google, Twitter et Mozilla) ont signé le Code de bonnes pratiques contre la désinformation de la Commission européenne, dans lequel ils s'engagent à prendre des mesures spécifiques pour empêcher que la désinformation permette de manipuler les citoyens de l'Union européenne. Dans le monde entier, les plateformes de médias sociaux telles

que Facebook, Instagram, Google, Youtube et Twitter sont invitées à faire preuve de davantage de transparence au sujet du suivi et du ciblage des internautes et à leur donner plus de contrôle sur leurs propres données.

Partout, des préoccupations émergent à propos de l'avenir. En Afrique, 19 pays vivront des élections en 2019. En Asie, ce sera le cas dans plus de 10 pays. L'Amérique latine connaîtra neuf élections, dont six présidentielles. Une couverture des événements responsable et des informations factuelles représentent des éléments clés pour que les citoyens puissent choisir de manière éclairée les personnes qui devraient gouverner. Ainsi, la lutte contre la désinformation s'avère essentielle, même si elle ne doit pas ébranler la liberté d'expression ni le libre accès à l'information. Lorsque le pouvoir est en jeu, aucune dépense n'est épargnée pour influencer l'opinion publique ou museler les critiques.

Lectures complémentaires

Our Data, Ourselves: Politics and Data, Tactical Tech, 2019

Digital Deceit: The Technologies Behind Precision Propaganda on the Internet, Dipayan Ghosh, Ben Scott, New America, 2018

A multi-dimensional approach to disinformation, Independent high level group on fake news and online disinformation, Commission européenne, 2018

Elections – Global Voices en français

Qui veille sur les données de vos enfants ?

Crédit photo : Kelly Sikkema sur Unsplash

Nous expliquons aux enfants qu'ils ne doivent pas faire confiance aux étrangers qu'ils rencontrent dans l'espace public. Pourtant, bien trop souvent, les parents eux-mêmes donnent à des étrangers accès à la vie de leurs enfants par Internet.

Les enfants d'aujourd'hui devront composer avec un nombre inégalé de traces numériques. En fait, certains sont associés à des données avant même leur naissance, car les parents téléchargent des échographies sur Internet et les professionnels du marketing ne cessent de traquer les femmes enceintes. Difficile de prédire les effets sur les individus, mais lorsque les parents et les personnes qui s'occupent des enfants enregistrent les étapes importantes de la vie de ces derniers dans des applications, suivent leurs déplacements et diffusent leur vie sur les réseaux sociaux, leur identité numérique devient une mine d'informations.

Un rapport publié en 2018 par le Commissaire anglais pour l'enfance, intitulé *Who knows what about me*, a révélé qu'en moyenne un habitant du Royaume-Uni compte 70 000 publications en ligne à son sujet au moment de ses 18 ans. Pour souligner les risques que cela entraîne, la banque Barclays prévoit que les informations partagées en ligne par des parents au sujet de leurs enfants causeront deux tiers des

usurpations d'identité et des escroqueries financières auxquelles seront confrontés les jeunes d'ici fin 2030.

De plus, les enfants eux-mêmes grandissent et découvrent en ligne des informations qui les concernent et qu'ils souhaiteraient pouvoir effacer. En exemples, nous pouvons citer l'adolescente autrichienne qui a poursuivi ses parents pour avoir partagé des centaines de photos d'elle (y compris aux toilettes) avec leurs 700 contacts sur les réseaux sociaux et l'élève de quatrième année de primaire qui a demandé à sa mère, chroniqueuse, d'arrêter de partager ses histoires et photos privées.

« Les adolescents reçoivent beaucoup d'avertissements sur le fait que nous ne sommes pas assez mûrs pour comprendre que tout ce que nous publions en ligne est indélébile, mais les parents devraient aussi réfléchir à leur utilisation des réseaux sociaux et au possible impact sur la vie de leurs enfants lorsque nous deviendrons de jeunes adultes », écrivait une jeune Américaine de 14 ans qui a déclaré qu'elle allait quitter les réseaux sociaux, après avoir été embarrassée et s'être sentie trahie par les publications de sa mère et de sa sœur à son sujet depuis sa naissance.

Les Nations Unies ont réclamé l'adoption de « directives strictes » pour protéger la vie privée des enfants. En France et en Italie, les tribunaux se sont rangés du côté de l'enfant plutôt que de ses parents dans les affaires de partage de détails intimes sans le consentement de l'enfant. Quelles autres mesures peuvent être prises ?

Les gouvernements peuvent fixer des limites quant au type de collecte de données et de marketing acceptable au sujet d'enfants. En Europe, par exemple, le Règlement général sur la protection des données (RGPD) impose désormais des règles plus strictes sur la manière dont les données relatives aux enfants peuvent être collectées et traitées.

Les écoles ont un rôle à jouer pour enseigner aux élèves et à leur famille à naviguer dans un univers numérique tout en préservant leur vie privée. Ensuite, les développeurs d'applications et les plateformes web peuvent établir des lignes directrices claires en matière de protection de la vie privée afin que les parents (et les enfants eux-mêmes) soient en mesure d'évaluer les avantages et les inconvénients de l'utilisation des services et des jeux en ligne.

Enfin, les personnes qui gardent des enfants peuvent être attentives aux appareils et jouets dotés d'une connexion Internet qui entrent dans la vie de ces enfants. En effet, certains appareils écoutent les conversations et capturent des données de manière pernicieuse.

Toutefois, la solution la plus simple tient dans le fait de réfléchir à deux fois avant de publier quoi que ce soit au sujet de votre enfant. Le contenu en question pourra-t-il être vu par ses futurs amis ou employeurs ? Un Internet sain se caractérise par un environnement dans lequel nous nous sentons à l'aise avec les informations partagées qui nous concernent et concernent notre famille, que nous soyons enfants ou adultes.

Lectures complémentaires

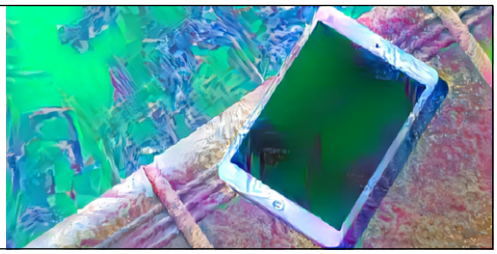
Who Knows What About Me? Children's Commissioner for England, 2018

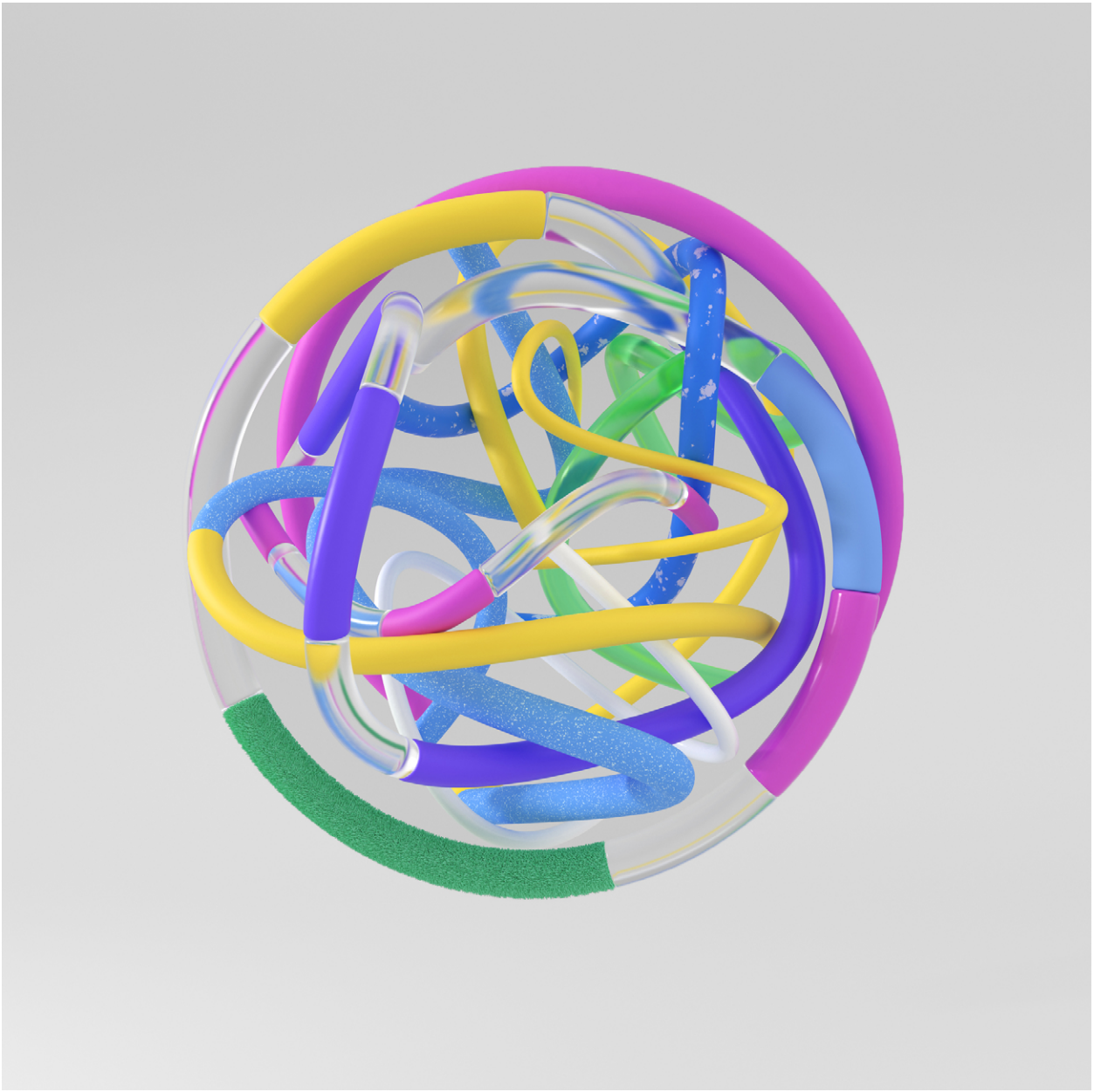
I'm 14, and I quit social media after discovering what was posted about me, Fast Company, 2019

Sharenting: Children's Privacy in the Age of Social Media, Stacey B. Steinberg, Levin College of Law, Université de Floride, 2017

YouTube Is Improperly Collecting Children's Data, Consumer Groups Say, New York Times, 2018

Plus de contenu disponible en ligne

Décoder les images de la guerre en Syrie	
Détecter la surveillance de masse grâce à la réalité virtuelle	
Se libérer de la dépendance aux appareils	



Décentralisation Introduction

Qui contrôle Internet ?

Une poignée de grands acteurs dominent une grande partie du monde en ligne, mais Internet bénéficie d'une meilleure santé lorsqu'il est contrôlé par le plus grand nombre.

Bon nombre des défis que rencontre la santé d'Internet aujourd'hui peuvent être attribués au fait que les produits et les services numériques les plus répandus sont contrôlés par une petite poignée d'acteurs.

Au cours de l'année passée, le débat sur cette consolidation du pouvoir s'est poursuivi, aiguisé et, dans certains cas, enflammé.

Huit entreprises américaines et chinoises dominent le monde numérique : Alphabet (holding de Google), Alibaba, Amazon, Apple, Baidu, Facebook, Microsoft et Tencent.

Ces sociétés et leurs filiales détiennent un contrôle démesuré sur Internet. Elles dominent tous les aspects du monde numérique, des moteurs de recherche, navigateurs et services de médias sociaux que beaucoup d'entre nous utilisent quotidiennement, jusqu'aux infrastructures de base comme les câbles sous-marins et l'informatique à distance, invisible pour la plupart des utilisateurs. Ils ont bâti leurs empires sur la vente de notre attention aux annonceurs, le bouleversement des modèles économiques, la création de nouveaux marchés en ligne et la conception de matériel et de logiciels désormais profondément intégrés dans la vie de beaucoup d'entre nous. Leur influence ne cesse de croître, dans notre vie privée comme dans l'espace public. Aussi, leurs faux-pas peuvent réellement causer du tort.

Dans l'écosystème d'Internet, un bon équilibre du pouvoir requiert des interactions délicates entre les gouvernements, les entreprises et la société civile. Nous avons besoin de normes efficaces relatives à la concurrence et d'interopérabilité entre les produits de *différentes* entreprises pour garantir qu'Internet se développe et évolue de manière à répondre aux divers besoins des citoyens du monde entier.

Les amendes pour infraction aux lois sur la concurrence, comme l'amende de 5 milliards de dollars infligée à Google par les autorités de réglementation de l'Union européenne en 2018, n'ont pas eu l'effet nécessaire pour garantir un avenir équilibré et ouvert.

Beaucoup explorent de nouvelles solutions pour faire évoluer Internet dans une voie qui ne soit pas tracée par les intérêts des géants du secteur. Nous voyons émerger de nouveaux modèles économiques qui cherchent à distribuer le contrôle parmi les utilisateurs, dont les plateformes coopératives et les modèles de propriété collective.

Des communautés dynamiques d'innovateurs œuvrent à proposer de nouvelles solutions pour se détourner des systèmes centralisés, en s'appuyant sur l'amélioration de la connectivité locale, sur le développement de projets, de protocoles et de produits décentralisés et sur la création d'espaces de publication hors des grandes plateformes technologiques.

Dès le début, Internet a permis de défier l'autorité, de remettre en question les modèles économiques traditionnels et d'offrir plus de transparence, d'ouverture et de responsabilité. Mais cette vision fondée sur la force perturbatrice au service du bien ne peut pas être tenue pour acquise.

Chaque internaute est concerné par les enjeux de son avenir, des autorités municipales aux experts techniques, en passant par la génération des internautes de demain.

Pour bénéficier d'un Internet qui offre de véritables choix, nous devons soutenir les produits qui diversifient le marché ainsi que les lois et les politiques qui protègent les utilisateurs et favorisent une saine concurrence. Nous devons unir nos forces et encourager l'action citoyenne, la recherche et l'innovation afin de bâtir un Internet plus sain.

Décentralisation Données

Comment les plus grandes sociétés Internet réalisent leurs bénéfices

Huit entreprises exercent un pouvoir énorme sur l'ensemble d'Internet : Google, Facebook, Microsoft, Amazon, Apple, Baidu, Alibaba et Tencent. Aujourd'hui, la plupart des internautes utilisent au moins l'une d'elle au quotidien.

Elles possèdent chacune tellement de produits, de services et d'investissements différents qu'il s'avère parfois compliqué d'identifier leur principale source de revenus ou de comprendre comment une entreprise tire profit des services qu'elle propose « gratuitement », tels que les recherches, les messageries électroniques, les jeux, les médias sociaux ou les messageries instantanées.

Comment ces mastodontes du Net gagnent-ils de l'argent ? Nous les avons classés en quatre catégories qui se recoupent en fonction de leur principale source de revenus.

Lectures complémentaires

Des entreprises technologiques trop grandes ?, Bulletin de santé d'Internet 2018

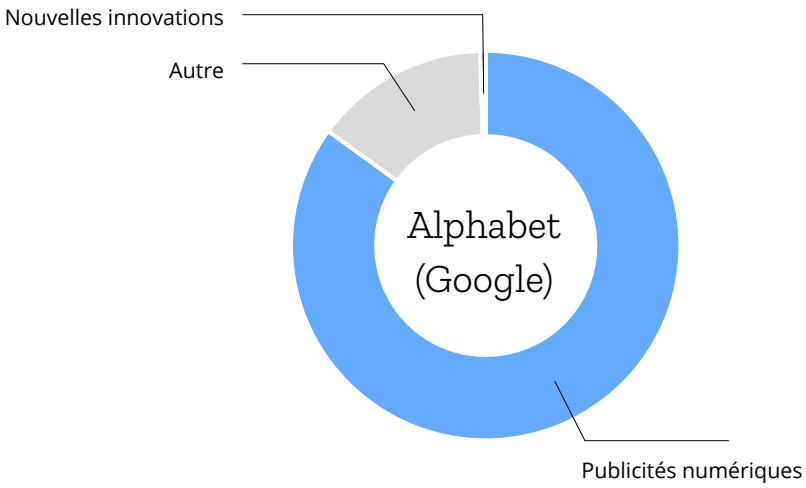
'Big Tech' isn't one big monopoly – it's 5 companies all in different businesses, The Conversation, 2018

Tencent, the $500bn Chinese tech firm you may never have heard of, The Guardian, 2018

Breaking Down How Amazon Makes Money, Visual Capitalist, 2017

Les marchands d'attention : Google, Facebook et Baidu

Vendre votre attention rapporte de l'argent. La spécialité de Google, Facebook et Baidu consiste à collecter des données sur vos activités en ligne et permettre aux éditeurs et aux spécialistes du marketing de vous cibler avec des annonces personnalisées. En 2018, Google et Facebook contrôlaient à eux deux environ 84 % du marché mondial de la publicité numérique hors de Chine.

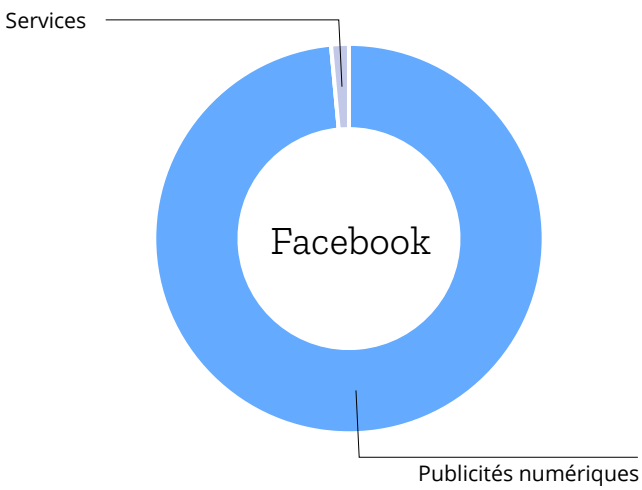


Alphabet (Google)
Alphabet, la société mère de Google, tire 85 % de ses revenus de la publicité numérique. Environ 70 % proviennent d'annonces diffusées sur les produits de Google, par exemple le moteur de recherche Google Search ou YouTube. Alphabet possède également Google AdSense et Google AdMob, des services de placement d'annonces sur d'autres sites, qui comptent ensemble pour 14,6 % de ses revenus. Les ventes d'appareils, comme les téléphones, les assistants à domicile et les applications de Google Play représentent 14,5 % des revenus d'Alphabet.

Chiffre d'affaires (2018)
136,8 milliards (USD)

Capitalisation boursière
795,3 milliards (USD)

Sources:
Rapport annuel 2018, Alphabet, 2019.
Estimation de la capitalisation boursière de Yahoo Finance, le 4 mars 2019

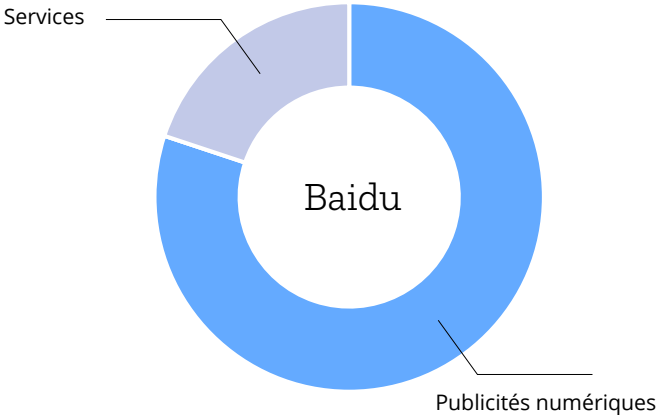


Facebook
Nous considérons Facebook comme un « réseau social », pourtant il s'agit d'une agence de publicité. Avec environ 2,32 milliards d'utilisateurs actifs mensuels, Facebook tire plus de 98,5 % de son chiffre d'affaires, soit plus de 55 milliards de dollars, de la vente de publicités qui s'affichent dans nos fils d'actualité, principalement dans l'application Facebook. Une fraction de ses revenus (1,5 %) provient des jeux et d'autres applications et produits vendus sur Facebook.

Chiffre d'affaires (2018)
55,8 milliards (USD)

Capitalisation boursière
463,1 milliards (USD)

Sources:
Rapport annuel 2018, Facebook, 2019.
Estimation de la capitalisation boursière de Yahoo Finance, le 4 mars 2019



Baidu
Baidu possède le premier moteur de recherche de Chine, qui représente plus de 70 % de parts de marché. Ses revenus et son développement sont inférieurs à ceux de Google, mais l'entreprise suit un modèle économique similaire. Baidu tire environ 80 % de ses revenus de la vente de publicités. Une source de revenus moins importante (environ 20 %) provient des abonnements à iQIYI (un service de vidéos en continu semblable à Netflix) et des services de paiement. Comme Alphabet, Baidu investit également dans l'intelligence artificielle et dans d'autres innovations, comme les voitures autonomes.

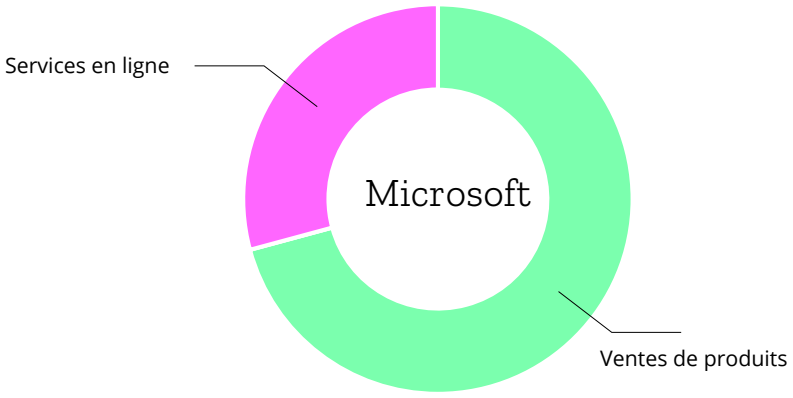
Chiffre d'affaires (2018)
14,9 milliards (USD)

Capitalisation boursière
56,6 milliards (USD)

Sources:
Rapport annuel 2018, Baidu, 2019.
Estimation de la capitalisation boursière de Yahoo Finance, le 4 mars 2019

Les machinistes : Apple et Microsoft

Microsoft et Apple tirent la majeure partie de leurs revenus de la création et de la vente d'appareils et de logiciels qui nous donnent accès au monde en ligne. Les téléphones mobiles, les ordinateurs, les consoles de jeux, ainsi que les logiciels comme les programmes de traitement de texte et de stockage en ligne, constituent tous des produits qui génèrent des revenus.

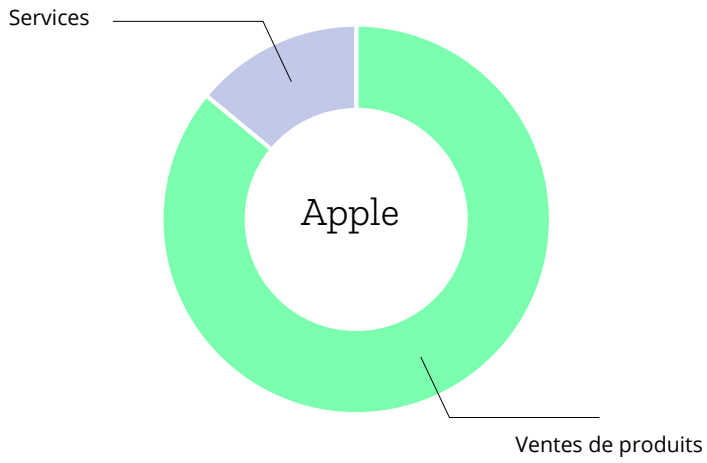


Microsoft
70,8 % du chiffre d'affaires de Microsoft provient de la vente de produits de différentes catégories, y compris des outils de « productivité » comme les logiciels Microsoft Office et la plateforme de recrutement en ligne LinkedIn. Ces ventes de produits comprennent aussi les logiciels (y compris Windows), le matériel (y compris les tablettes Xbox et Surface) et les publicités liées à son moteur de recherche. Les services en ligne de Microsoft ont généré 29,2 % de son chiffre d'affaires total en 2018.

Chiffre d'affaires (2018)
110,4 milliards (USD)

Capitalisation boursière
863,4 milliards (USD)

Sources:
Rapport annuel 2018, Microsoft, 2018.
Estimation de la capitalisation boursière de Yahoo Finance, le 4 mars 2019



Apple
Apple tire 86 % de ses revenus de la vente d'appareils numériques et d'ordinateurs. L'iPhone règne en maître puisque plus de la moitié du chiffre d'affaires total d'Apple en 2018, soit près de 167 milliards de dollars, provient de la vente du coûteux téléphone mobile. Les ventes d'ordinateurs Mac représente 9,6 % des ventes de produits et celles de l'iPad, 7 %. Les services d'Apple, notamment iCloud, Apple Care ou Apple Pay, comptent pour 14 % du chiffre d'affaires général de l'entreprise.

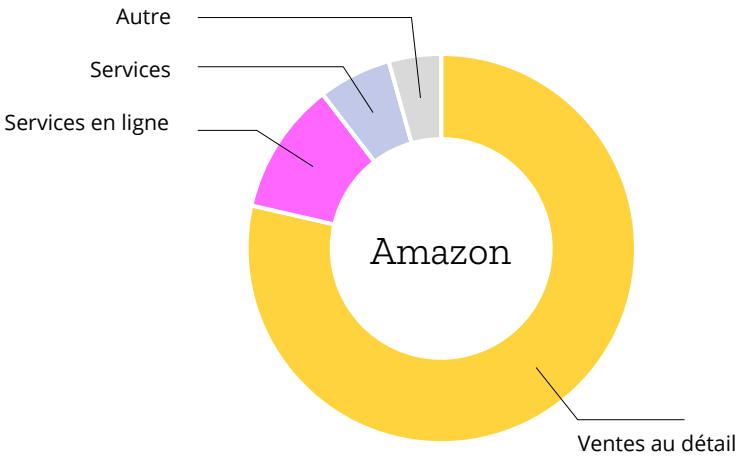
Revenue (2018)
265,6 milliards (USD)

Market capitalization
825,0 milliards (USD)

Apple Source:
Rapport annuel 2018, Apple, 2018.
Estimation de la capitalisation boursière de Yahoo Finance, le 4 mars 2019

Les intermédiaires du commerce de détail : Alibaba et Amazon

Amazon et Alibaba tirent principalement leurs revenus de la vente de produits en ligne. Amazon et Alibaba ouvrent désormais également des succursales physiques qui complètent l'expérience en ligne. Ils ne s'arrêtent pas là : ils vendent aussi des publicités et des services numériques, tels que la diffusion de vidéo en direct, le soutien logistique et l'informatique dans le cloud ou encore les transactions financières et même la livraison de repas!

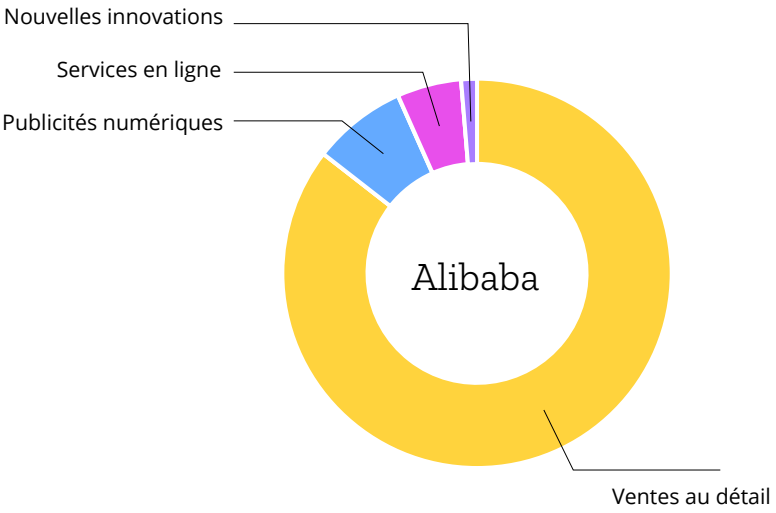


Amazon
Si à l'origine, il s'agissait d'un commerce de livres, désormais, Amazon vend de tout. L'entreprise tire la majeure partie de ses revenus (78,5 %) des ventes au détail. Les abonnements à Amazon Prime (y compris la diffusion vidéo en continu) représentent 6 % de ses revenus. Amazon Web Services, un service en ligne à la demande qui offre de la puissance de calcul, le stockage de bases de données, l'hébergement web et d'autres fonctionnalités, représentait 11 % du chiffre d'affaires total d'Amazon en 2018.

Chiffre d'affaires (2018)
232,9 milliards (USD)

Capitalisation boursière
821,2 milliards (USD)

Sources:
Rapport annuel 2018, Amazon, 2019.
Estimation de la capitalisation boursière de Yahoo Finance le 4 mars 2019



Alibaba
Alibaba réalise l'essentiel de son chiffre d'affaires (85,6 %) en vendant des produits à 552 millions de clients en Chine, mais également en proposant des publicités numériques, des abonnements à Youku Todou (un service populaire de diffusion vidéo en direct) et des services en ligne. Alibaba investit dans l'intégration et la numérisation de ses différentes activités. De plus, Alibaba innove avec des produits logiciels comme AutoNavi, un service de cartographie qui compte environ 60 millions d'utilisateurs actifs par jour.

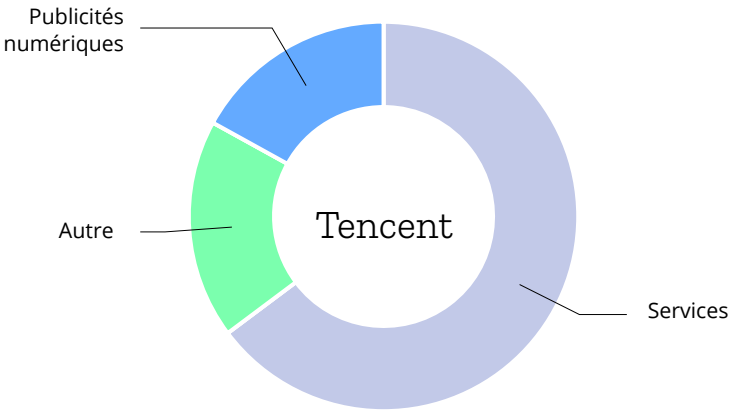
Chiffre d'affaires (2018)
39,9 milliards (USD)

Capitalisation boursière
476,7 milliards (USD)

Sources:
Rapport annuel 2018, Alibaba, 2018.
Estimation de la capitalisation boursière de Yahoo Finance le 4 mars 2019

L'entreprise multifacettes : Tencent

La société chinoise Tencent est surtout connue pour sa plateforme de messagerie WeChat, mais l'entreprise ne révèle pas combien celle-ci lui rapporte directement. Contrairement à WhatsApp ou Telegram, WeChat représente bien plus qu'une application de messagerie: le service, profondément intégré à la vie quotidienne en Chine, vous permet par exemple de payer vos factures et de prendre rendez-vous chez le médecin.



Tencent
La majorité des revenus de Tencent provient d'achats virtuels dans les applications (principalement dans les jeux) et des abonnements sur Tencent Video (regroupés dans les « Services », avec 56,6 % du total des revenus en 2018). Le domaine des services de paiement occupe une place toujours plus importante (inclus dans « Autre », avec 24,9 %) principalement sous forme de commissions sur les transactions en ligne via WeChat Pay. De plus, Tencent tire des revenus des publicités numériques sur ses plateformes médiatiques et applications de messagerie (18,5 %).

Chiffre d'affaires (2018)
45,5 milliards (USD)

Capitalisation boursière
397,2 milliards (USD)

Sources:
Rapport annuel 2018, Tencent, 2019.
Estimation de la capitalisation boursière de Yahoo Finance le 4 mars 2019

Décentralisation Personnes

Et si Facebook appartenait à ses utilisateurs ?

Pendant des décennies, les fondateurs de start-up ont considéré les possibilités que leur offrait Internet avec des dollars dans les yeux. Dans une culture d'entreprise nourrie par de grands apports de capital-risque, les start-up rivalisent pour devenir la prochaine à décoller et générer des profits à faire des envieux, comme Uber ou WhatsApp.

Trop souvent, les modèles économiques des plus grandes entreprises d'Internet les ont amenées à piétiner la confiance des utilisateurs et des employés en plaçant les profits avant l'intérêts général.

Au plus fort des scandales publics, des utilisateurs ont lancé des campagnes comme #DeleteUber ou #DeleteFacebook pour exprimer leur désapprobation. Toutefois, le manque de solutions de qualité pour se détourner des géants du Web comme Amazon, Google ou Facebook rend peut-être l'abandon de ces services trop prohibitif au niveau social et économique. Pouvons-nous envisager une voie véritablement démocratique qui permettrait aux utilisateurs de piloter des entreprises ?

Une nouvelle génération d'entrepreneurs du numérique émerge pour relever ce défi. Par exemple, nous pouvons citer Zebras Unite, un mouvement dirigé par des femmes pour promouvoir des solutions plus éthiques et inclusives que celles proposées par la culture des

Nathan Schneider. Photo de Emily Hansen (CC BY-SA 4.0).

« licornes », les grandes start-up du secteur technologique. Ou la Purpose Foundation qui fait la promotion du modèle du *steward-ownership* pour donner la priorité à la mission plutôt qu'au profit. De plus, des centaines d'entreprises structurées et gérées de façon coopérative à travers le monde explorent des méthodes de partage du pouvoir et des profits directement avec les utilisateurs, afin de briser le cycle de maximisation du gain à tout prix.

Répertorier ces différentes formes d'entrepreneuriat numériques ou de « plateformes coopératives » passionne Nathan Schneider, de l'Université du Colorado à Boulder (États-Unis). Avec Trebor Scholz, instigateur du Platform Cooperative Consortium de la New School de New York, il a coorganisé certains des premiers rassemblements des membres de ce type de communautés. Auteur de Everything for Everyone: The Radical Tradition That Is Shaping the Next Economy, Nathan Schneider a de plus cofondé Start.coop, un accélérateur d'entreprises pour les nouvelles coopératives.

Q : À quels problèmes les plateformes coopératives pourraient-elles répondre ?

R : L'économie en ligne connaît une crise majeure en matière de responsabilité. Les entreprises se substituent à certains services publics et nous n'avons pas le choix d'utiliser ou non leurs services par manque d'autres solutions valables. Certains utilisateurs s'inquiètent des données qu'ils communiquent, mais s'avouent impuissants devant l'absence de choix. La propriété collective représente une opportunité d'intégrer la responsabilisation des plateformes. Pour les utilisateurs, cela constitue un moyen de se faire entendre et d'injecter de la démocratie dans les entreprises. Et, peut-être même de conduire à un rajeunissement de la sphère démocratique.

Le plus souvent, les gens n'envisagent même pas la possibilité de créer des nouvelles solutions pour remplacer les entreprises existantes dont l'offre ne tient pas compte des intérêts des utilisateurs.

En 2016, lorsqu'Uber a quitté Austin, au Texas, à la suite d'un différend avec les autorités locales, un nouveau système de transport partagé, Ride Austin, a vu le jour. Le service, plus intéressant pour les chauffeurs, soutient en outre des organismes à but non lucratif locaux. Il offre une vision totalement différente des possibilités de fonctionnement dans une économie.

Q : Vous semble-t-il envisageable que les grandes entreprises du secteur technologique évoluent vers des modèles coopératifs ?

R : Ne serait-il pas formidable que ces grandes entreprises appartiennent aussi aux utilisateurs qui génèrent leur réelle valeur ? Au lieu de cela, l'économie en ligne génère des profits énormes pour un petit nombre d'actionnaires. Considérer les utilisateurs comme des partenaires à part entière leur assure de ne pas être exclus de la valeur qu'ils créent et de bénéficier, tout comme les investisseurs, de la richesse produite collectivement.

En 2017, j'ai participé à une campagne qui visait à présenter une résolution d'actionnaires lors d'une assemblée annuelle de Twitter afin d'encourager l'entreprise à envisager des options pour élargir la propriété et la gouvernance de la plateforme aux utilisateurs afin de résoudre des problèmes systémiques. Cette tentative n'a pas porté ses fruits, mais nous devons multiplier les stratégies pour promouvoir la démocratie dans les entreprises. Surtout quand nous reconnaissons qu'elles atteignent des tailles qui les transforment en services publics. Par exemple, une structure juridique et des régimes fiscaux pourraient amener quelqu'un comme Mark

Zuckerberg, dirigeant de Facebook, à considérer comme une option raisonnable la possibilité de transférer de grandes quantités d'actions et de contrôle aux utilisateurs.

Q : L'attrait du financement par capital-risque est fort. Cela dit, qu'est-ce qui motive les fondateurs d'un projet à se tourner plutôt vers un modèle d'entreprise coopératif ?

R : Souvent, les gens essaient de résoudre des problèmes de fond et se rendent compte que les confier aux investisseurs ne suffira pas. Prenons, par exemple, Jen Horonjeff, fondatrice de Savvy, une plateforme d'information sur la santé pour les patients et leurs familles. Atteinte d'une maladie chronique, elle était obnubilée par l'idée que les patients puissent mieux contrôler leur maladie. Toutefois, elle savait que chaque fois que des procédés médicaux sont confiés à des investisseurs, les patients finissent par être exploités. Elle s'est donc tournée, en dernier recours, vers un modèle coopératif de manière à protéger les utilisateurs, tout en dirigeant une entreprise.

L'économie a besoin de diversité. Le modèle classique à haut risque et à fort rendement du capital-risque sera peut-être toujours nécessaire, mais son existence n'empêche pas la création de davantage d'options.

Lectures complémentaires

Ours to Hack and to Own: The rise of platform cooperativism, a new vision for the future of work and a fairer Internet, édité par Nathan Schneider et Trebor Scholz, 2017

Platform Cooperative Consortium

The Internet of Ownership Website and Directory

Why the cooperative models need to be at the heart of our new economy, Fast Company, 2018

Décentralisation Analyse

Quand un ouragan balaie Internet

Loiza, Porto Rico, six mois après l'ouragan Maria. Photo de Preston Keres (domaine public).

Internet est conçu pour faire preuve de résilience. Mais, après l'ouragan Maria de 2017, lorsque les Portoricains ont voulu prendre des nouvelles de leurs proches, beaucoup ont découvert qu'ils ne pouvaient pas se connecter.

La tempête avait brisé des lignes électriques et renversé des tours de télécommunications. Les infrastructures de télécommunication, détruites à 95,6 %, ont laissé les habitants en quête de signal. L'ouragan avait anéanti Internet.

Cette catastrophe a endommagé un demi-million de bâtiments et tué des milliers de personnes. Selon certaines estimations, elle a causé la pire coupure de courant de l'histoire des États-Unis [NdT : Porto Rico est un territoire « non incorporé » des États-Unis].

Les conditions météorologiques extrêmes causées par le changement climatique augmentent la probabilité que de telles catastrophes se reproduisent bientôt – à Porto Rico et ailleurs dans le monde – et qu'une fois de plus les coupures d'Internet rendent une crise humanitaire encore plus difficile à surmonter.

« Nous parlons d'êtres humains [qui ont perdu la vie] à cause des télécommunications, parce qu'il était impossible de décrocher le téléphone ou d'envoyer un message », a déclaré la journaliste portoricaine Sandra Rodriguez dans une interview avec NOVA Next au sujet des coupures d'Internet.

Après l'ouragan Maria, les problèmes de connexion se sont rapidement propagés au-delà de Porto Rico. Plusieurs pays d'Amérique du Sud qui dépendent des câbles sous-marins qui traversent l'île des Caraïbes, dont l'Argentine et le Brésil, ont connu des interruptions de réseau en septembre 2017 en raison de pannes de courant.

Les initiatives, déployées à petite et à grande échelle, dans le but de restaurer Internet se sont multipliées. L'organisme à but non lucratif NetHope a envoyé et installé des équipements Wi-Fi. Les entreprises de télécommunications ont déployé des points d'accès mobiles. Le projet Loon de Google a proposé une connexion Internet au moyen de ballons stratosphériques. Pourtant, près d'un an a été nécessaire pour rétablir l'alimentation électrique de toute l'île et les vitesses de connexion moyennes n'ont pas atteint les niveaux antérieurs à la tempête avant août 2018, selon NOVA Next.

Chaque année, à l'approche de la saison des ouragans, les défenseurs portoricains d'Internet réclament des mesures afin de renforcer Internet pour faire face à la prochaine grosse tempête. En février 2018, l'Internet Society (ISOC), une organisation à but non lucratif qui défend l'accès à Internet pour tous, a publié un rapport avec les informations de ses antennes caribéennes sur les mesures possibles pour tenter d'empêcher une autre catastrophe en matière de connectivité.

L'électricité représente une ressource incontournable. Mais la géographie naturelle et la planification historique de l'île rendent l'approvisionnement énergétique difficile. Par exemple, alors que la plupart des 3,3 millions d'habitants de Porto Rico vivent dans les zones métropolitaines du nord, 70 % de l'électricité est produite dans le sud. Cette centralisation maladroite signifie que le réseau doit traverser l'île, exposant ainsi les lignes électriques aux intempéries.

La distribution de l'électricité dans les montagnes de Porto Rico s'avère également difficile et coûteuse. Après la coupure de courant, les tours de téléphonie cellulaire ont dû compter sur des générateurs de secours. Une fois le carburant épuisé, « il était impossible d'atteindre les tours parce que les routes étaient bloquées, alors les antennes ont arrêté de fonctionner, faute d'alimentation. C'était compliqué. », a déclaré Eduardo Diaz, directeur du comité de l'antenne portoricaine d'ISOC, qui participe à la formation d'un comité consultatif pour aider à élaborer le plan stratégique de cette antenne.

Selon M. Diaz, au niveau local, la perte de confiance dans le réseau électrique favorise l'émergence de nouvelles solutions énergétiques durables et décentralisées mieux adaptées au climat. « C'est une île tropicale où le soleil brille la grande majorité de l'année… Vous n'imaginez pas le nombre de personnes qui souhaitent se tourner vers le solaire ou ne pas dépendre du réseau au cas où une telle situation se reproduirait. Le marché est colossal » indique M. Diaz.

Mais Porto Rico doit aussi sensibiliser les acteurs du secteur Internet aux problèmes climatiques. En effet, malgré le fait que la région soit exposée aux tempêtes, le secteur ne construit pas toujours de façon durable.

Shernon Osepa, responsable des affaires régionales pour l'Amérique latine et les Caraïbes de l'ISOC, estime qu'il est nécessaire de résoudre ce problème. « Ces opérateurs savent que nous

vivons dans un environnement très vulnérable, mais certains déploient des réseaux comme s'ils intervenaient dans une région où de tels phénomènes climatiques ne se produisent pas », explique M. Osepa, soulignant que certaines infrastructures des Caraïbes ne peuvent résister qu'à des ouragans de catégorie 3, alors que la région connaît des ouragans de catégorie 4 et 5.

Ouvrir les données au public constitue une étape clé pour la reprise. « Nous ne disposons pas d'une vue complète du mauvais état des télécommunications », explique M. Diaz. Il déclare que le groupe de travail sur le haut débit de Porto Rico devrait en priorité cartographier les parties de l'île qui ne bénéficient pas d'une connexion haut débit.

Porto Rico souffre d'infrastructures défaillantes et de restrictions budgétaires depuis bien avant la tempête. L'Agence fédérale des situations d'urgence (FEMA) des États-Unis a contribué des sommes importantes aux réparations d'urgence, mais les politiciens hésitent à fournir les fonds nécessaires à une refonte complète des infrastructures. Au lieu de cela, ils optent pour des solutions rapides, voire des projets qui portent atteinte à l'intérêt de Porto Rico.

Face aux limites budgétaires, Eduardo Diaz encourage la réflexion créative et les solutions plus durables. Il mentionne par exemple les subventions en faveur de l'accès à Internet pour les écoles publiques qui pourraient servir à créer des « institutions d'ancrage », lesquelles aideraient à fournir une connexion aux membres des communautés environnantes.

Le changement climatique favorise l'apparition de nouveaux obstacles pour les défenseurs d'Internet dans les Caraïbes et le reste du monde. Il ne fait aucun doute que le nombre d'ouragans et de catastrophes naturelles augmentera. Ainsi, il est urgent de déployer dès aujourd'hui de nouveaux types d'infrastructures, adaptées aux différentes régions.

Lectures complémentaires

Report from the Field: Post-Hurricane Connectivity in the Caribbean, Internet Society, février 2018

After Hurricane Maria, Puerto Rico's Internet Problems Go from Bad to Worse, NOVA Next, octobre 2018

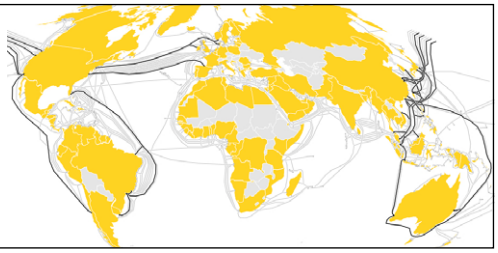
Lights Out: Climate Change Risk to Internet Infrastructure, University of Wisconsin – Madison, 2018

Puerto Rico's Slow Internet Recovery, Oracle Internet Intelligence, 2017

Décentralisation

Plus de contenu disponible en ligne

Les câbles sous-marins attirent de nouveaux investisseurs



Une solution open source pour les services en ligne

10 minutes pour un Internet plus sain

Quelques suggestions pour améliorer dès maintenant la santé de votre Internet :

1. Vérifier les paramètres de confidentialité de vos applications

Les applications représentent des outils idéaux pour jouer, se déplacer en ville et rester en contact avec des amis. Cependant, elles en savent aussi beaucoup sur vous et peuvent communiquer des données à votre sujet. Vous pouvez vérifier les réglages de confidentialité de vos applications Android préférées sur AppCensus AppSearch pour en savoir plus sur les données auxquelles elles accèdent et qu'elles partagent avec d'autres parties sur Internet.

2. Protéger vos comptes

La sécurité de vos données personnelles dépend de celle de vos mots de passe.

Vérifiez si votre compte a été exposé. Si c'est le cas, cessez d'utiliser le mot de passe compromis et changez-le partout, même pour vos anciens comptes. Si le risque concerne vos données bancaires, avertissez votre banque et surveillez vos relevés.

Protégez-vous en utilisant un mot de passe différent pour chaque compte. Un gestionnaire de mots de passe comme 1Password, LastPass, Dashlane et Bitwarden peut vous aider en générant des mots de passe complexes et en les mémorisant tous pour vous.

Activez l'authentification à deux facteurs partout où cette option est disponible. Pour recevoir des informations en cas de fuite de données qui affecterait votre compte, inscrivez-vous à l'alerte Firefox Monitor.

3. Réfléchir à deux fois avant de réaliser un test ADN

Faire analyser un échantillon de votre ADN comporte des répercussions sur la protection de votre vie privée, mais aussi sur celle des membres de votre famille. Dans la mesure du possible, discutez avec les personnes concernées des répercussions sur la protection de la vie privée de chacun, de la probabilité que le test donne des résultats exacts, et planifiez des solutions pour vous aider à vous confronter à d'éventuelles surprises.

Rejoindre le mouvement

Il existe de nombreux organismes et groupes dans le monde, et probablement aussi dans votre pays ou votre ville, qui œuvrent à améliorer la santé d'Internet. S'impliquer dans une organisation représente souvent le meilleur moyen d'en apprendre davantage et de contribuer à la création d'un Internet plus sain.

Les organisations que nous mentionnons dans le rapport de cette année sont un excellent point de départ. Nous vous suggérons des façons d'entrer en contact avec certaines d'entre elles ci-dessous. Il vous suffit de répondre à la question suivante : que voulez-vous faire ?

Vous êtes également invités à vous impliquer avec Mozilla, l'organisation qui publie le Bulletin de santé d'Internet. Vous trouverez ici des possibilités pour vous engager.

Je souhaite apporter mon aide

→ **Soutenez et apportez votre contribution à Wikimedia** : un mouvement mondial qui a pour mission de proposer un contenu éducatif gratuit au monde. Il est probablement principalement connu pour son encyclopédie en ligne gratuite, Wikipédia. Cependant, il développe d'autres projets, comme Wikidata. Il existe de nombreuses façons de s'impliquer, notamment en identifiant l'antenne locale la plus proche de vous.

→ **Aidez Access Now à lutter contre les coupures d'Internet en rejoignant la campagne #KeepItOn.** Les coupures de réseau connaissent une augmentation : Access Now a documenté 188 blocages dans le monde en 2018, soit plus du double qu'en 2016. Avec #KeepItOn, Access Now recueille et partage des témoignages à propos de l'incidence des coupures d'Internet sur la vie des individus, et réunit des soutiens pour exiger que les dirigeants mondiaux s'engagent à garantir l'accès à Internet

Je souhaite apporter mon aide

Pour un Internet ouvert

→ **Soutenez et apportez votre contribution à Wikimedia** : un mouvement mondial qui a pour mission de proposer un contenu éducatif gratuit au monde. Il est probablement principalement connu pour son encyclopédie en ligne gratuite, Wikipédia. Cependant, il développe d'autres projets, comme Wikidata. Il existe de nombreuses façons de s'impliquer, notamment en identifiant l'antenne locale la plus proche de vous.

→ **Aidez Access Now à lutter contre les coupures d'Internet en rejoignant la campagne #KeepItOn.** Les coupures de réseau connaissent une augmentation : Access Now a documenté 188 blocages dans le monde en 2018, soit plus du double qu'en 2016. Avec #KeepItOn, Access Now recueille et partage des témoignages à propos de l'incidence des coupures d'Internet sur la vie des individus, et réunit des soutiens pour exiger que les dirigeants mondiaux s'engagent à garantir l'accès à Internet

Pour un Internet plus privé et plus sûr

→ **Établissez un relais pour le projet Tor,** un navigateur gratuit qui permet aux internautes de publier et de partager des informations en ligne avec un haut niveau de confidentialité et de sécurité. En soutenant Tor, vous aiderez à défendre l'anonymat en ligne pour des millions de personnes dans le monde.

→ **Rejoignez l'Internet Society**, une organisation qui aide à instaurer et à soutenir des communautés qui font fonctionner Internet et dont la mission vise à créer un Internet connecté au niveau mondial, sécurisé et digne de confiance. Regardez s'il existe une antenne de l'Internet Society dans votre région. Si ce n'est pas le cas, envisagez d'en constituer une.

Pour un Internet inclusif

→ **Prenez part à l'Algorithmic Justice League pour aider à combattre les biais et à accroître la responsabilisation des systèmes automatisés.** Fondée par Joy Buolamwini, l'Algorithmic Justice League mène des recherches sur des sujets comme la façon dont les systèmes commerciaux d'analyse faciale intègrent des biais sexistes et racistes, et propose des solutions telles que le Safe Face Pledge : un guide pour aider les entreprises à mettre au point une technologie d'analyse faciale qui ne nuit pas aux individus.

→ **Devenez un TrollBuster** Lorsque vous identifiez des menaces en ligne, des comportements qui relèvent du cyberharcèlement ou d'autres types d'agissements imputables à des trolls à l'encontre de femmes jounalistes, signalez-les à TrollBusters. L'organisation vous enverra, à vous ou à la personne ciblée, des messages positifs, des câlins virtuels ou des services de réparation de réputation. Près des deux tiers des femmes journalistes interrogées par TrollBusters et l'International Women's Media Foundation en 2018 ont déclaré avoir été victimes de harcèlement en ligne.

Pour une meilleure éducation au Web

→ **Aidez à améliorer la lisibilité des Conditions d'utilisation avec le projet** Terms of Service; Didn't Read (ou « ToS;DR »). « J'ai lu et j'accepte les conditions générales » constitue l'un des plus gros mensonges sur le Web. ToS;DR vise à remédier à cela. Les contributeurs du projet lisent et évaluent les conditions d'utilisation, dans le but de pousser les entreprises à faire en sorte que les utilisateurs comprennent plus facilement les dispositions qu'ils acceptent.

→ **Découvrez comment soutenir les décodeurs d'Amnesty International pour soutenir la recherche sur les droits humains.** Il s'agit d'une communauté de plus de 50 000 bénévoles dans plus de 150 pays qui offrent leur temps et leurs compétences en ligne. Entre les mains des défenseurs des droits humains qui œuvrent à protéger les personnes vulnérables dans le monde entier et à demander justice pour elles, Internet constitue un puissant outil de documentation. Les projets des décodeurs sont divisés en micro-tâches auxquelles n'importe qui peut participer.

Pour un Internet décentralisé

→ **Faites don de votre voix au projet Common Voice.** Common Voice a été fondée afin de promouvoir une innovation plus décentralisée, en aidant à rendre les données nécessaires à la création de systèmes de reconnaissance vocale ouvertes et accessibles à tous. Cette initiative représente désormais le plus grand ensemble de données vocales humaines prêtes à être utilisées.

→ **Envisager d'autres modèles économiques pour Internet.** Explorez des communautés comme le Platform Cooperativism Consortium, des projets comme The Internet of Ownership ou Zebras Unite, un mouvement dirigé par des femmes pour promouvoir des solutions plus éthiques et inclusives que la culture des « licornes » de la Silicon Valley.

moz://a mzl.la/ihr-fr