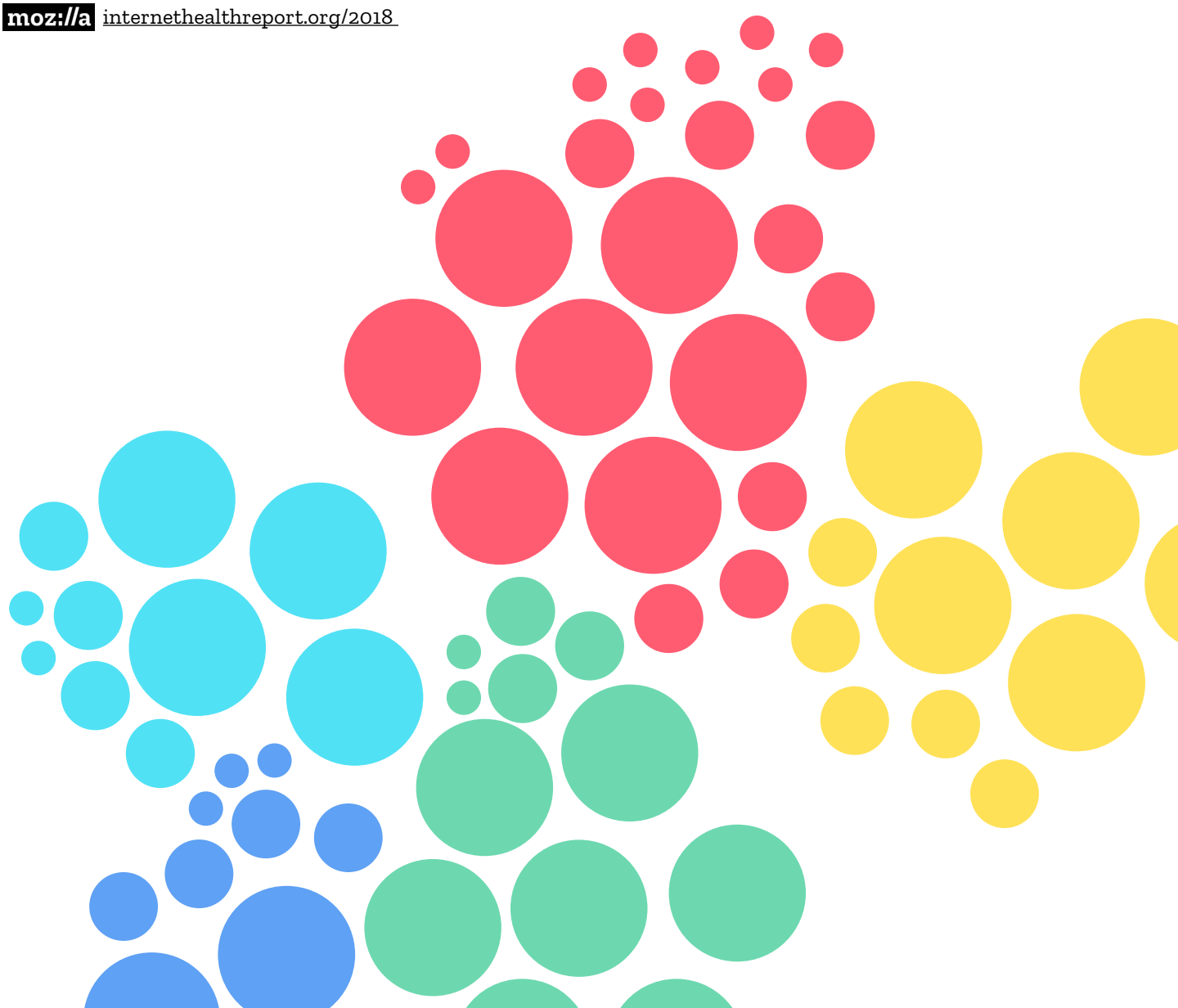
Bulletin de santé d'Internet 2018

Le Bulletin de santé d'Internet 2018 constitue une compilation d'études et présente les éléments qui participent au développement d'Internet et ceux qui lui nuise, selon cinq thèmes.

moz://a internethealthreport.org/2018



Index

README

Le Bulletin de santé d'Internet s'intéresse à la dimension humaine de l'accès et de l'utilisation d'Internet. Il s'agit d'une compilation indépendante et à code source ouvert de données, d'études et de récits qui présente chaque année l'évolution d'Internet considérée selon cinq perspectives.

Vous connaissez peut-être d'autres rapports à propos d'Internet qui traitent plus directement des tendances de ce secteur et des nouvelles technologies. Tel n'est pas notre objectif.

En collaboration avec des chercheurs, des activistes des droits numériques, des bénéficiaires d'une bourse de Mozilla et notre communauté, nous racontons une histoire collaborative sur ce qui est sain et ne l'est pas au sujet d'Internet, d'un point de vue humain.

Ce rapport s'appuie sur un large éventail d'études consacrées à des questions allant du respect de la vie privée à la connectivité, en passant par le harcèlement en ligne et la dimension économique des plateformes web.

Il vise à établir des liens et à rechercher d'éventuelles tendances entre des sujets souvent cloisonnés, pour étudier la relation entre les internautes et Internet.

Ainsi, nous souhaitons encourager une compréhension plus large de la façon dont les problèmes qui touchent Internet à l'échelle mondiale sont liés les uns aux autres, et mettre en lumière les actions des citoyens pour améliorer la santé de cet écosystème.

Nous tous avons la possibilité d'améliorer Internet. Ce rapport constitue une ressource ainsi qu'un appel à l'action pour toutes les personnes prêtes, par de petits et de grands gestes, à relever ce défi.

Les différents éléments de ce rapport peuvent être lus dans n'importe quel ordre et nous vous encourageons, après chaque lecture, à réagir et à discuter de son contenu.

Un prototype de ce rapport a été publié en janvier 2017, puis a donné lieu à des discussions ouvertes et publiques sur les indicateurs, à plusieurs réunions avec nos soutiens et à la création d'une plus petite « coalition du rapport» pour aider à en produire le contenu. Vous pouvez aussi lire les mises à jour du projet sur notre blog.

Consultez : Internet Health Report v. 0.1

Remerciements

De nombreux chercheurs, confrères, rédacteurs et soutiens de Mozilla ont généreusement fourni des données et des idées. En outre, d'innombrables lecteurs nous ont fait part de leurs commentaires au cours du processus.

Éditrice : **Solana Larsen**
Chef de projet : **Kasia Odrozek**
Chargé de diffusion : **Jairus Khan**
Pour nous contacter, écrire à :
internethealth@mozillafoundation.org

Nous remercions nos amis de Vizzuality pour la conception visuelle et interactive, le codage ainsi que les essais utilisateurs. Le Bulletin de santé d'Internet et le blog sont disponibles en anglais, en français, en espagnol et en allemand. Les traductions ont été réalisées par des membres de Global Voices.

Découvrez la liste complète des contributeurs en ligne.

Comment se porte Internet ?

Il devient plus facile d'expliquer en quoi consiste la santé d'Internet, comparé à l'année passée quand nous avons lancé le prototype du Bulletin de santé d'Internet. Qu'est-ce qui a changé ?

D'une part, les gros titres ont continuellement souligné les aspects malsains d'Internet. Beaucoup ont commencé à s'inquiéter de la trop grande domination des entreprises technologiques. Les médias sociaux ont servi d'instruments de harcèlement. Nos informations personnelles ont été dérobées et les processus démocratiques ébranlés par la manipulation des médias et des publicités en ligne.

Pas étonnant que 2017 ait été considérée comme « une année terrible pour la technologie » par certains.

Les nouveautés : Un nombre croissant de personnes comprend l'incidence réelle d'Internet sur nos sociétés, nos économies et notre bien-être personnel. Nous commençons à considérer la santé d'Internet non seulement comme un problème technique, mais aussi humain.

Telle est l'approche adoptée par le Bulletin de santé d'Internet et la raison pour laquelle il examine un large éventail de facteurs afin d'évaluer l'écosystème dans son ensemble.

Ce rapport présente des informations et des perspectives du monde entier sur cinq thèmes : vie privée et sécurité, ouverture, inclusion numérique, éducation au Web et décentralisation.

Nous avons également mis en lumière trois des plus grands problèmes de santé d'Internet de l'année dernière : la sécurité de l'Internet des objets, la désinformation et la taille des entreprises technologiques. L'immersion dans ces thèmes montre comment un sujet habituellement restreint peut offrir une vue d'ensemble.

Dans le texte sur la taille des entreprises technologiques, nous explorons comment les entreprises dominantes des États-Unis et de la Chine créent des conditions malsaines pour les innovateurs en difficulté et les populations moins nombreuses qui essaient de percer le marché, et pour un scientifique qui tente de sortir des filets de Google. La consolidation des pouvoirs dans le secteur technologique ne répond pas uniquement à une question d'affaires, elle soulève aussi des interrogations tant au niveau géopolitique que personnel. Que souhaitons-nous pour Internet ?

Avec Comprendre l'écosystème de la désinformation, nous nous détachons de la Russie et de l'élection américaine de 2016 et étudions les raisons pour lesquelles la désinformation en ligne s'est convertie en une préoccupation mondiale. Vous voulez un indice ? Le marché de la publicité en ligne va mal, dans le sens où il se plie facilement à la fraude et aux abus. Au-delà des propagandistes, le texte évoque aussi ces adolescents qui gagnent facilement de l'argent grâce aux publicités en ligne et les personnes qui partagent des propos incendiaires, parce qu'ils ne connaissent encore rien de mieux pour l'instant.

Enfin, la cybersécurité est souvent présentée comme un problème relatif aux hackers, pourtant elle est aussi étroitement liée à la santé de l'écosystème d'Internet dans son ensemble. D'ici 2020, le monde comptera jusqu'à 30 milliards d'appareils connectés, y compris des webcams non sécurisées, des Babyphones et d'autres appareils pouvant être asservis et utilisés collectivement comme une arme. La sécurisation de l'Internet des objets représentera ainsi un défi qui implique la correction des mauvaises pratiques relatives aux logiciels, au matériel et à la gouvernance qui fragilisent Internet. Qui devons-nous tenir pour responsable ? Comment trouver des solutions significatives pour maintenir un Internet en bonne santé et sûr ? Nous aurons besoin de réponses multiples.

Ce qui nous ramène à la question : **quel est l'état de santé d'Internet ?** De manière générale, il ne s'agit pas d'une question simple. Certes, il existe quelques indicateurs faciles à surveiller. Les choses s'améliorent dans des domaines comme l'accès, l'abordabilité, le chiffrement. Toutefois, ils empirent dans d'autres comme la censure, le harcèlement en ligne et la consommation d'énergie. Cependant, ces indicateurs simples ne traduisent pas la complexité des écosystèmes mondiaux comme Internet.

Nous devons prêter attention aux contractions, comme la tension croissante entre la liberté d'expression et le harcèlement. Nous devons surveiller les technologies et les acteurs qui, même s'ils revêtent une importance moindre aujourd'hui, pourraient prendre une ampleur considérable demain, comme les fabricants d'appareils à code source ouvert ou les innovateurs de la chaîne de blocs. Il nous faut penser de manière créative à la façon dont les personnes qui conçoivent la technologie, l'utilisent et les la réglementent peuvent collaborer à créer un monde numérique véritablement enrichissant pour tous.

Dans le monde, nous sommes toujours plus nombreux à nous exprimer, à partager des connaissances et à concevoir des produits dans le but de relever ces défis. Pour tous ceux qui essaient de rendre le monde numérique meilleur, nous espérons que le Bulletin de santé d'Internet y apportera sa contribution, même minime.

Nous vous encourageons à explorer les différentes parties du Bulletin de santé d'Internet, à vous intéresser aux questions et à participer aux discussions.

N'hésitez pas à nous contacter et à nous faire part de vos idées. Ce rapport représente une initiative collaborative, à code source ouvert et notre équipe attache de l'importance à tout commentaire ou remarque.

La sécurisation de l'Internet des objets

Quelque part au Vietnam, un homme cherche une boîte à chaussures dans une arrière-boutique ; une femme tranche du pain en Argentine et un enfant s'assoit sur les genoux de sa mère dans la salle d'attente de ce qui ressemble à une pharmacie française. Au même moment, une vache passe à la traite en Allemagne.

Tous sont filmés par des caméras de sécurité accessibles en ligne sans mot de passe. Ils ne se doutent sûrement pas qu'ils peuvent être observés par quiconque recherche des caméras non sécurisées sur Internet. La personne chargée de configurer la caméra aurait pu choisir de restreindre l'accès avec un mot de passe, mais sans cette protection, le contenu est accessible en ligne, aucun piratage n'est nécessaire.

Considérez maintenant que le nombre d'appareils connectés devrait doubler entre 2015 et 2020, pour atteindre 30 milliards. Chaque dispositif dépourvu de mot de passe ou doté d'un mot de passe faible rend Internet un peu plus vulnérable et dangereux. Malgré cela, les consommateurs achètent des appareils, les connectent à Internet et ne pensent jamais à les sécuriser, tant qu'ils fonctionnent.

Moniteurs d'activité physique, appareils de cuisine, ampoules… Cette année, nous serons écoutés, observés, reconnus et enregistrés par des téléphones, des assistants numériques et des caméras comme jamais auparavant.

Les données ainsi recueillies peuvent faire l'objet de piratages ou de fuites. Nous pourrions nous préoccuper des individus déséquilibrés à la recherche d'images de personnes nues qui ne soupçonnent pas que de telles images d'elles sont vues, d'arnaques financières, de publicités envahissantes ou de manipulations politiques, mais ce n'est pas tout… Les voitures partagent-elles nos habitudes de conduite avec les compagnies d'assurance ? Les aspirateurs commercialisent-ils des informations relatives à l'aménagement de nos foyers ? Pour la plupart des gens, ces risques demeurent hypothétiques et peinent à peser plus lourd dans la balance que le plaisir de tirer profit de l'Internet des objets.

En réalité, la « surface d'attaque » d'Internet augmente et nous avons déjà eu un avant-goût des conséquences désagréables.

En décembre 2017, trois jeunes hommes ont plaidé coupables devant un tribunal fédéral américain pour avoir créé, en 2016, une génération de logiciels malveillants appelée Mirai afin d'asservir des milliers de webcams, des Babyphones et autres appareils qui utilisaient les noms d'utilisateur et les mots de passe par défaut paramétrés en usine, de manière à mener des attaques par déni de service (DDoS) pour bloquer des sites web et des réseaux. Pour dissimuler leur identité, les auteurs ont partagé le code de ces logiciels et ainsi provoqué la multiplication des réseaux de bots informatiques de Mirai qui ont commencé à se faire concurrence (et le font toujours) pour contrôler les appareils à travers le monde. Ils ont réussi à bloquer temporairement certaines parties d'Internet aux États-Unis et en Europe, à travers une attaque à grande échelle contre l'entreprise Dyn, une importante société de gestion de serveurs DNS. En Europe, des banques et des fournisseurs d'accès Internet ont ainsi été victimes d'extorsions, de même qu'une université au New Jersey.

Offrir des « services de sécurité », qui étaient en réalité des extorsions voilées, faisait partie du plan initial sournois des auteurs de Mirai, tout comme accumuler des dollars grâce à la création de faux trafic sur les publicités en ligne au moyen de réseaux de bots informatiques. À l'époque, certains experts en sécurité soupçonnaient des acteurs gouvernementaux comme la Chine ou la Russie de tester la résilience d'Internet. Les véritables responsables se sont révélés moins menaçants, mais les risques que posent tous ces « objets » non

sécurisés existent toujours et s'intensifient avec chaque nouvel appareil connecté.

Bien que le battage médiatique se concentre sur les gadgets et les appareils ménagers connectés, parmi les secteurs les plus concernés par l'Internet des objets, nous pouvons citer la santé, les transports, l'énergie et les services publics. La technologie offre de formidables opportunités d'améliorer l'efficacité et la qualité des services publics, de santé et des infrastructures.

En outre, le matériel informatique peu coûteux et la décentralisation de l'innovation fournissent un accès Internet à un nombre croissant de personnes,

sous des formes plus diverses que jamais. Si cela constitue une raison de se réjouir, malheureusement dans la société actuelle du jetable, les appareils connectés sont rarement conçus pour offrir une sécurité satisfaisante sur la durée.

Puisque tous les logiciels deviennent vulnérables aux attaques ou aux dysfonctionnements au fil du temps, les mises à jour logicielles automatiques s'avèrent indispensables. Cependant, cela restera plus compliqué pour les petites entreprises qui vendent des appareils connectés à bas prix et ne possèdent pas les ressources et l'expertise de sociétés comme Google, Apple ou Amazon.

À qui demander des comptes lorsque la relation entre le fabricant et le consommateur se distingue par une telle opacité ? Pourrions-nous imaginer des règlements et des codes de conduite destinés à l'industrie qui garantiraient l'utilisation de mots de passe forts, aléatoires et uniques sur les appareils connectés ? Des dispositifs de sécurité techniques permettraient-ils de former un bouclier autour du réseau de l'Internet des objets d'une personne ? Pourquoi ne pas considérer la création de labels de fiabilité pour l'IoT, à l'instar des étiquettes pour l'alimentation bio ou les appareils économes en énergie ? Quel rôle peuvent jouer les concepteurs ? Ces idées, et beaucoup d'autres, doivent être étudiées, explorées et discutées en 2018.

Le problème clé provient du fait que l'Internet des objets croît plus vite et davantage que nous l'aurions imaginé. Certains risques concernent la sphère personnelle (par exemple le possible embarras ou les blessures que pourrait vous infliger une voiture piratée), alors que d'autres concernent le système ou l'environnement (comme la neutralisation d'un hôpital ou d'un réseau électrique). Quoi qu'il en soit, résoudre ce type de problème s'avérera coûteux lorsque les choses tourneront mal.

Actuellement, le terrain le plus réactif pour la sensibilisation reste les foyers : se comporter en consommateurs plus intelligents, en particulier en tant que parents pour protéger les enfants contre les jouets non sécurisés qui contiennent des microphones cachés, des caméras ou d'autres enregistreurs de données personnelles. Des poupées comme « Hello Barbie » et « My Friend Cayla » qui écoutent et parlent aux enfants ont fait la Une, car elles peuvent très facilement faire l'objet de piratage. D'ailleurs, l'Allemagne a interdit Cayla, qu'elle considère comme un « dispositif de transmission caché ». Il existe probablement d'autres possibilités de tirer parti de la réglementation existante de protection des consommateurs.

Nous devons nous préoccuper sérieusement de la façon dont nous traitons ces problèmes en tant que société, de la part que nous pouvons laisser à l'industrie, de celle qui relève du choix des consommateurs et de celle qui nécessite une réglementation.

Pour en savoir plus :

Predictions for Journalism 2018, News Games Rules, Mariano Blejman, 2017

How a Dorm Room Minecraft Scam Brought Down the Internet, WIRED, 2017

A Trustmark For IoT, Peter Bihr, ThingsCon, 2017

Privacy Not Included, An IoT Buyer's Guide, Mozilla, 2017

Une réaction à la lecture de cet article ?

Comprendre l'écosystème de la désinformation

Confronter les personnes au pouvoir à la vérité a déjà valu des ennemis à Filip Stojanovski. Dans le cadre de son poste de directeur du programme de la fondation macédonienne Metamorphosis, Filip Stojanovski a contribué à la création du Media Fact-Checking Service, un organisme de surveillance des médias, ainsi qu'à plusieurs autres projets qui favorisent la connaissance « ouverte » et la démocratie en ligne. Pourtant, il a trouvé absurde de voir des publications Facebook sponsorisées avec de fausses affirmations à son sujet en 2015.

« Pour moi, aucun doute, il s'agit d'une campagne de propagande contre les personnes qui refusent de garder le silence sur les problèmes dans ce pays. ». Cependant, il ne sait toujours pas qui l'a financée.

En revanche, Filip Stojanovski est conscient qu'elle s'inscrivait dans une plus large campagne qui visait à intimider et à dénigrer les organisations de la société civile en Macédoine.

Ce type d'embuscades dans les médias sociaux a pris des proportions épidémiques à travers le monde, en partie parce que l'économie de la publicité en ligne, sur laquelle repose une grande partie du Web moderne, va mal. Exception faite de la politique locale, la hausse de la désinformation discutée sous la bannière fourre-tout du moment, les fakes news, doit être appréhendée dans le contexte des réalités malsaines du marché qui peuvent récompenser un comportement malveillant à des fins lucratives ou politiques.

Actuellement, la majorité de la population s'informe, au moins partiellement, sur les médias sociaux. Afin d'optimiser les revenus générés par la publicité, les flux d'actualités affichent les contenus susceptibles d'attirer l'attention du plus grand nombre. Cette méthode favorise ainsi les titres qui appellent des réactions, soit des mentions « j'aime » ou des commentaires. Ajoutez à cela la possibilité d'améliorer la visibilité de n'importe quel message par l'achat d'une « annonce » pour cibler les personnes les plus enclines à réagir (selon leurs intérêts, comportements et relations), de diffuser de fausses informations à une vitesse incroyable et de suivre leur progression. Si seulement la réalité était aussi excitante que la fiction…

La palette des protagonistes à l'origine de la désinformation va d'individus malveillants à simplement opportunistes, avec des cibles aussi bien locales que mondiales. Ensuite, les personnes qui transmettent, partagent et propagent les contenus (pour autant qu'il s'agisse d'êtres humains et non de robots) ne possèdent pas de caractéristiques qui les unissent. Chacun est susceptible d'y participer, même si les extrémistes y sont plus enclins, peut-être du fait de l'indignation que leur inspirent nombre de différents sujets que d'autres ne perçoivent pas comme des faits avérés.

Aux États-Unis, des scandales liés à de fausses informations (dont celui sur un réseau pédophile supposément piloté par des proches d'Hillary Clinton qui sévirait dans une pizzeria) ont entaché l'élection présidentielle américaine de 2016 et les questions sur le rôle joué par la désinformation dans l'élection de Donald Trump ne sont pas encore résolues. Les activistes russes sont les principaux protagonistes de cette enquête, basée sur des preuves évidentes qu'une organisation liée au Kremlin, Internet Research Agency, a dépensé des centaines de milliers de dollars pour alimenter le Web de propos politiques toxiques, avant et après les élections.

Dans ce cas, la réalité n'a rien à envier à de la fiction.

Les Russes ont créé des dizaines de « fausses » pages Facebook, comme « BlackMattersUS » et « Heart of Texas » qui imitent les discours de divers contextes politiques aux États-Unis. Ils ont attiré des milliers

d'abonnés et utilisé lesdites pages pour organiser des manifestations réelles et même, à une occasion, une manifestation et une contre-manifestation en même temps.

De nombreux titres des médias ont été consacrés aux liens entre la Russie et les États-Unis, mais un tel comportement n'est pas spécifique à la Russie. Dans de trop nombreux pays, et cela dans les démocraties aussi bien que dans les États autoritaires, les gouvernements, les militaires et les partis politiques utilisent Internet pour manipuler l'opinion publique à l'échelle nationale ou à l'étranger sous de faux prétextes. Ils emploient des proxys et déploient des trolls, des bots logiciels et d'autres techniques qui visent à masquer leur identité.

Les Macédoniens sont eux-mêmes plutôt familiers de l'ingérence russe. Toutefois, les combats contre la désinformation dans ce pays datent de bien avant Internet.

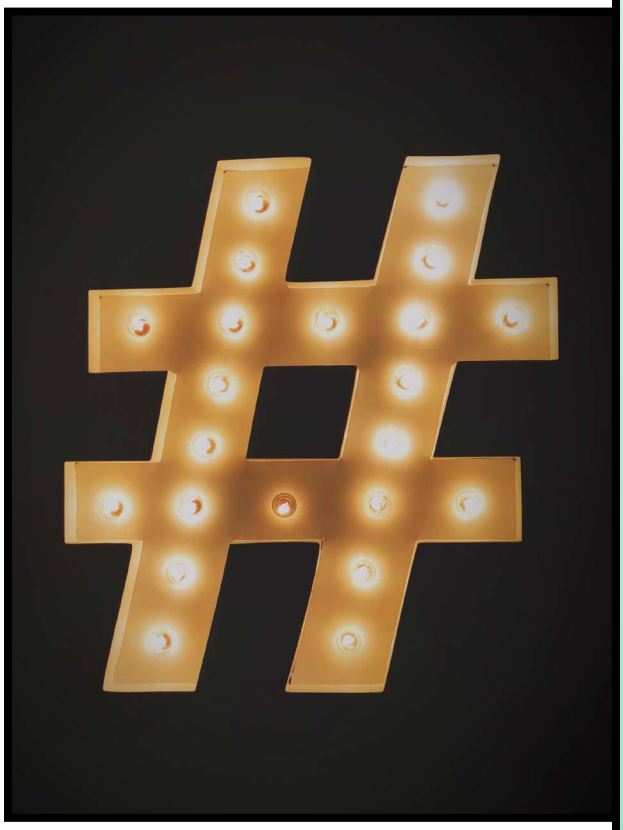
Filip Stojanovski estime que les décennies de propagande gouvernementale, qui a marqué les différentes étapes du conflit et la transition politique du socialisme à la démocratie en Macédoine ont désabusé les citoyens. La désinformation caractérise la façon dont l'opinion publique est façonnée, dit-il, parce que les médias traditionnels travaillent directement au service des partis populistes.

Cet écosystème particulier pour la vérité, les mensonges et la politique a offert un terrain fertile à une industrie artisanale de « fausses informations » en Macédoine, qui ont également fait une brève apparition dans la campagne présidentielle des États-Unis.

Les journalistes d'investigation de différents pays (dès six mois avant le jour de l'élection américaine) ont retracé les origines de milliers de contenus à caractère désinformatif dans une petite ville de Macédoine appelée Veles, autrefois connue pour sa porcelaine. Les jeunes habitants ont créé des centaines de sites web avec des gros titres en anglais conçus pour recueillir les dollars tirés des publicités numériques. Ils imaginent des sites web sur tous les sujets, de la santé et du sport à la finance et plus encore.

Quels contenus ont-ils jugé les plus lucratifs ? Les articles au sujet de Donald Trump. Au moyen des mêmes mécanismes que ceux décrits ci-dessus, les adolescents macédoniens ont réussi à exploiter « l'économie de l'attention ». D'un point de vue réaliste, ils utilisent les mêmes dynamiques qui font de Trump le principal sujet des grands médias numériques traditionnels étasuniens. Les internautes cliquent, les annonces rapportent de l'argent et plus d'articles sont rédigés.

La désinformation en ligne constitue une menace majeure pour la santé d'Internet et de toutes les



sociétés qu'elle touche en raison du risque de désordre politique, de discréditation de la vérité, de la haine et des rumeurs qui se propagent dans les conflits ou lors de catastrophes, mais également à cause des tentatives de rapides rectifications des politiciens (avec ou sans arrière-pensées) qui peuvent menacer l'ouverture d'Internet.

Par exemple, face aux questions de désinformation et de discours haineux en ligne, l'Allemagne a décidé d'attribuer aux plateformes de médias sociaux la responsabilité de supprimer les contenus illégaux. D'autres pays, y compris la Russie et le Kenya, ont ensuite adopté des lois dans ce sens. Cependant, nous devrions nous méfier des solutions qui investissent Facebook, Twitter ou d'autres sociétés (ou leurs algorithmes) du rôle de gardiens d'Internet.

Au lieu de chercher des solutions rapides, nous devons prendre le temps de mieux comprendre le problème ainsi que le kaléidoscope des acteurs et des symptômes. Nous sommes confrontés à un mélange d'informations de pacotille, de propagande computationnelle, de pollution de l'information et de faible niveau d'éducation au Web.

De nombreuses personnes travaillent déjà sur les moyens de s'attaquer à certaines parties du problème. Les développeurs et les éditeurs tentent de construire des communautés plus réfléchies et équilibrées autour du sujet de l'information. La Credibility Coalition développe un standard web pour prendre en charge la détection de contenus moins sérieux et moins fiables. Les enseignants élaborent des programmes d'études pour aider leurs étudiants à lutter contre la désinformation et les réseaux sociaux essayent de rendre les publicités politiques plus transparentes, même si l'effet reste limité. Toutefois, la plupart de ces idées n'en sont qu'à leurs débuts.

Même si de tels efforts portent leurs fruits, beaucoup affirment que nous devrons encore nous attaquer à un problème de santé d'Internet plus important : le modèle sous-jacent de publicité et du taux de conversion en ligne qui récompense les abus, la fraude et la désinformation. Il est difficile d'imaginer le résoudre sans régulation, changements radicaux dans les modèles économiques d'Internet, ou les deux.

Pour autant, nous ne pouvons pas non plus tomber dans le piège qui consiste à blâmer la technologie pour les conditions sociales et économiques mondiales qui ont polarisé le débat politique, donné lieu à des médias éminemment partisans ou à d'autres facteurs très humains qui contribuent à ces problèmes.

Que les outils mêmes conçus pour le discours civique et le renforcement des communautés soient malmenés et discrédités joue précisément en faveur des individus qui préfèrent des sociétés fermées, moins de faits et un Internet moins sain.

Bien que ces questions soient vastes et complexes, il est essentiel de trouver des solutions, pour la santé d'Internet, et de nos sociétés. Si nous réussissons à les résoudre, tout en conservant la nature ouverte et favorable à la liberté d'expression d'Internet, nous aurons le potentiel de redynamiser la sphère publique. Dans le cas contraire, nous serons coincés dans un sacré pétrin.

Voilà la vérité.

Pour en savoir plus :

The Promises, Challenges, and Futures of Media Literacy, Data & Society, 2018

Why education is the only antidote to fake news, Huw Davies, New Statesman, 2018

Real News About Fake News, Nieman Lab

The Fake News Machine, CNN Money, 2017

Fake News and Cyber Propaganda: The Use and Abuse of Social Media, TrendMicro, 2017

Des entreprises technologiques trop grandes ?

Vous savez qu'une société Internet possède une taille démesurée lorsque vos amis vous considèrent comme un être bizarre pour avoir choisi de renoncer à ses services. En 2014, Chris Hartgerink en a eu assez de ce qu'il appelle la « surveillance d'entreprise ». Dans l'optique de protéger sa vie privée, il a entrepris un complexe processus qui a duré plus d'un an afin de dissocier sa vie de Gmail et Google. Quand Chris Hartgerink a informé tout le monde que pour le joindre, il faudrait bientôt passer par une adresse de messagerie chiffrée de ProtonMail, ses amis n'en ont pas cru leurs oreilles. Ils ont continué à lui demander pourquoi il changeait de service de messagerie.

« Cet aspect social rend l'abandon des services encore plus difficile », explique Chris Hartgerink, boursier chez Mozilla et candidat au doctorat en statistiques à l'Université de Tilburg, aux Pays-Bas. « Je suis persuadé que cela aurait empêché d'autres de prendre la même décision. »

Le contrôle du réseau par les principaux services Internet ne représente qu'une partie de l'emprise qu'ils exercent sur nos vies. En raison du volume de leurs avoirs, quelques entreprises comme Google, Facebook et Amazon (ou Baidu, Tencent et Alibaba si vous vivez en Chine) se sont insinuées non seulement dans notre vie quotidienne, mais aussi dans tous les aspects de l'économie mondiale, des discours civiques et de la démocratie elle-même.

Ces entreprises, nées des rêves des pionniers d'Internet, ont permis à des milliards de personnes de tous les horizons de tirer parti des avantages du Net. Elles ont contribué au développement de la communication, de la créativité et du commerce. Sans elles, nous disposerions de moins d'informations, d'une vitesse de connexion limitée, d'une efficacité plus basse et aurions bien moins d'occasions de rire !

Les contradictions se cachent dans la consolidation du pouvoir. Le problème ne tient pas au fait que ces entreprises pèsent des milliards de dollars, possèdent des centaines de millions d'utilisateurs ou de grands portefeuilles d'acquisition, mais bien à leur taille. Au moyen de pratiques commerciales monopolistiques propres à l'ère numérique, elles compromettent le respect de la vie privée, l'ouverture et la concurrence en ligne.

Les sociétés bénéficient d'un accès illimité à notre vie personnelle (essayez simplement de cacher une grossesse aux boutiques en ligne). Elles s'isolent de la concurrence et restreignent ainsi l'innovation. Comme leur capacité à analyser des quantités massives de données croît grâce aux progrès de l'intelligence artificielle et de l'informatique quantique, il est probable que leurs pouvoirs progressent également dans les domaines connexes grâce à des intégrations verticales dans le matériel, les logiciels, les infrastructures, les automobiles, les médias, les assurances et bien plus, sauf si nous trouvons un moyen de perturber leur développement ou d'y mettre un terme.

Comment ? Si vous supprimez votre compte Facebook demain, votre mère sera peut-être la personne la plus inquiète, mais l'avenir d'une entreprise fondée il y a seulement 14 ans n'est pas prédit. Les adolescents se lassent toujours plus de Facebook et son fondateur, Mark Zuckerberg, reconnaît maintenant, dans une année de mauvaise

presse, qu'ils ont besoin de nous pour sentir que « notre temps est bien employé ».

Les entreprises et les technologies peuvent changer, tout comme leur environnement réglementaire. La réglementation relative aux fusions et la loi sur la concurrence servent à lutter pour un Internet plus sain dans de nombreux pays. Cette année, le régulateur antitrust de l'Inde a infligé une amende de 21 millions de dollars à Google pour comportement portant atteinte à la concurrence (au terme d'une procédure lancée il y a sept ans).

L'année dernière, une amende encore plus lourde

de 2,8 milliards de dollars a été imposée à Google par la Commission européenne (dans le cadre d'une procédure également lancée sept ans plus tôt et qui a fait l'objet d'un appel). De plus, Facebook, Apple et Amazon ont tous fait l'objet d'enquêtes pour concurrence déloyale.

Ces actions montrent non seulement que les gouvernements peuvent jouer un rôle dans le rééquilibrage des pouvoirs, mais aussi à quel point nos systèmes antitrust sont lents et obsolètes. Il est nécessaire de les repenser pour qu'ils deviennent plus efficaces, à l'ère en rapide mouvement des marchés numériques et des effets de réseau.

Une véritable interopérabilité constituerait également un moyen efficace de rééquilibrer les pouvoirs et de favoriser la concurrence : imaginez que vous puissiez ouvrir WhatsApp et discuter avec un utilisateur de Signal. Une telle fonctionnalité pourrait stimuler la concurrence entre les services actuels et l'innovation parmi les nouveaux. L'interopérabilité pourrait en fin de compte devenir une condition usuelle imposée pour les futures fusions.

Si les utilisateurs contrôlaient leurs propres données et avaient la possibilité de les transférer librement vers d'autres services, cela réduirait les verrouillages et leur permettrait de passer d'un service de leur choix à un autre, y compris de se tourner vers des options qui ne comptent pas des centaines de millions d'utilisateurs. Ce principe de « portabilité des données » constitue une exigence du règlement général européen sur la protection des données (GDPR), qui entrera en vigueur en mai, sans que nous ne sachions encore comment il sera appliqué.

Nous avons pris l'habitude de profiter de services Internet gratuits et offrons, en échange, aux entreprises l'accès à nos données personnelles, qu'elles reconditionnent et revendent aux annonceurs numériques qui souhaitent cibler un public ou des comportements spécifiques.

Google et Facebook contrôlent 84 % du chiffre d'affaires publicitaire numérique mondial, en dehors de la Chine. Toutefois, ces sociétés n'ont pas manqué l'information selon laquelle 36 % des utilisateurs

d'ordinateurs de bureau utilisent désormais des bloqueurs de publicités pour éviter les publicités ennuyeuses, le traçage excessif, les logiciels malveillants, la mésinformation et la navigation web ralentie. Ils s'engagent dans des campagnes pour de « meilleures publicités », mais il est peu probable que des modèles publicitaires plus équitables en découlent.

Des niveaux similaires de consolidation caractérisent le premier marché Internet « indépendant » du monde : la Chine. Par exemple, WeChat, une application mobile de Tencent, connaît une telle omniprésence qu'elle entre en jeu dans pratiquement toutes les interactions en ligne. « C'est comme Facebook, WhatsApp, Instagram, Yelp, Square et Snapchat tout-en-un, avec une centaine d'autres applications », écrit Aman Agarwal dans une publication sur Hackernoon accompagnée de captures d'écran de l'application. Vous pouvez même naviguer sur Internet depuis l'application. Cette année, le pays procédera même à des essais avec les comptes WeChat afin de déterminer si ceux-ci pourraient fonctionner comme identification nationale électronique.

Beaucoup de nations (autoritaires et autres) regardent la Chine avec envie qu'elles considèrent comme l'un des rares pays qui a efficacement freiné l'ascension des entreprises de la Silicon Valley sur son territoire et permis aux alternatives locales de prospérer dans la nation qui compte le plus grand nombre d'internautes. Pourtant, la Chine ne représente qu'un nouvel exemple de ce à quoi ressemble la consolidation extrême des pouvoirs et de ce que pourrait apporter un avenir lointain avec des géants d'Internet encore plus puissants.

Dans le reste du monde, Facebook, Google et Amazon dominent Internet. Les pays en développement détiennent la plus petite part du marché mondial des applications et c'est là que les plaintes pour « colonialisme numérique » gagnent du terrain.

Si aucun moteur de recherche ne pourra jamais défier Google et qu'aucune application locale ne pourra jamais gagner une part de marché durable, les opportunités promises par un Internet gratuit et ouvert s'érodent. Les concurrents open source aux géants des médias sociaux, tels que Diaspora et Mastodon, sont rares et peuvent, au mieux, fournir une démonstration de la faisabilité pour d'autres futurs possibles à moins que les citoyens disposent de la possibilité de déplacer librement leurs données.

Les lois telles que le GDPR européen sont prometteuses sur des questions de portabilité des données par exemple, mais ne donneront pas de résultats significatifs à moins que les consommateurs formulent des exigences spécifiques aux entreprises et aux régulateurs. Même lorsque la loi est de notre côté, nous devons exprimer nos besoins : « Chères entreprises, voici comment je veux déplacer mes photos entre Facebook, Instagram et mon iPhone. »

La seule façon qu'Internet reste un bien commun exige de le réclamer, le façonner et le revendiquer. Les consommateurs, les gouvernements et les technologues doivent promouvoir une concurrence loyale, l'innovation ouverte, l'interopérabilité et des normes afin qu'Internet puisse évoluer de façon plus saine et plus humaine.

Pour en savoir plus :

OK Google: Delete My Account (No Wait. No Really.), Chris Hartgerink, 2018

Can Washington Stop Big Tech Companies? Don't Bet on It, Farhad Manjoo, New York Times, 2018

Competition through interoperability, Chris Riley, 2017

My Experiment Opting Out of Big Data Made Me Look Like a Criminal, Janet Vertesi, Time Magazine, 2014

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.

Nous partageons, consciemment ou non, plus d'informations personnelles que jamais auparavant.

Les principaux modèles économiques d'Internet reposent sur l'obtention du plus grand nombre d'informations possibles sur chacun, puis sur l'analyse, la réorganisation et la vente de ces informations. Ces gisements de données rendent possibles de nombreux nouveaux services, y compris l'apprentissage automatique des machines et la reconnaissance vocale. Cependant, cette collecte de données s'accompagne également d'un risque constant que les informations au sujet de notre vie sociale, notre situation financière, nos relations amoureuses ou nos opinions politiques fassent l'objet de fuites et nous exposent et nous portent préjudice.

En 2017, les nombreuses révélations relatives aux fuites de données (Equifax, Yahoo, Uber et bien d'autres) démontrent que beaucoup de sociétés à qui nous faisons confiance avec nos données ne se préoccupent pas assez de leur sécurité. À cela s'ajoutent les regards indiscrets des gouvernements.

La sécurité devient de plus en plus difficile à assurer à grande échelle. Chaque technologie, aussi bien logicielle que matérielle, présente de nouveaux risques. En 2017, le rançongiciel WannaCry a paralysé des cibles de haut niveau, y compris le système de santé publique britannique ; une faille dans les puces d'Intel a mis des millions d'appareils en péril ; des réseaux électriques ont été piratés en Ukraine et aux États-Unis.

Toutefois, les internautes ne comptent pas rester passifs et accepter ces risques. Ils créent des technologies pour protéger les infrastructures clés des attaques. Des équipes de cybersécurité bénévoles répondent aux urgences et les efforts de Cyberpeace se poursuivent face à la guerre mondiale de l'information.

Au fur et à mesure qu'Internet se développe et intègre davantage d'appareils connectés, le défi ne fait que croître. Nous avons atteint un point de non-retour : quand les maisons ont des appareils dotés de micros pour écouter, les centres commerciaux des caméras de reconnaissance faciale et les images satellites peuvent identifier nos voitures, pouvons-nous vraiment contrôler nos empreintes numériques ?

Malgré l'énormité de ces défis, il y a eu des progrès.

En Europe cette année, un nouveau règlement général sur la protection des données (GDPR) obligera les entreprises à respecter des dispositions strictes en matière de confidentialité et de consentement, élevant les exigences imposées aux détenteurs de données dans le monde entier. Un nombre croissant de personnes utilisent des techniques de sécurité comme l'authentification à deux facteurs, bien qu'elles représentent encore une minorité. Nous avons aussi constaté un recours croissant au chiffrement sur les messageries et dans le trafic web.

Dans les années à venir, nous devrions militer pour des lois globales sur la protection des données dans le monde entier et inciter les entreprises à prendre la sécurité au sérieux.

Et oui, nous devrions également choisir de meilleurs mots de passe…

Vie privée et sécurité // Données

Le chiffrement des sites web devient la norme

Le nombre de sites web chiffrés augmente rapidement. Près de 70 % du trafic de Firefox concerne désormais des pages web chargées au moyen du protocole HTTPS, contre seulement 50 % début 2017.

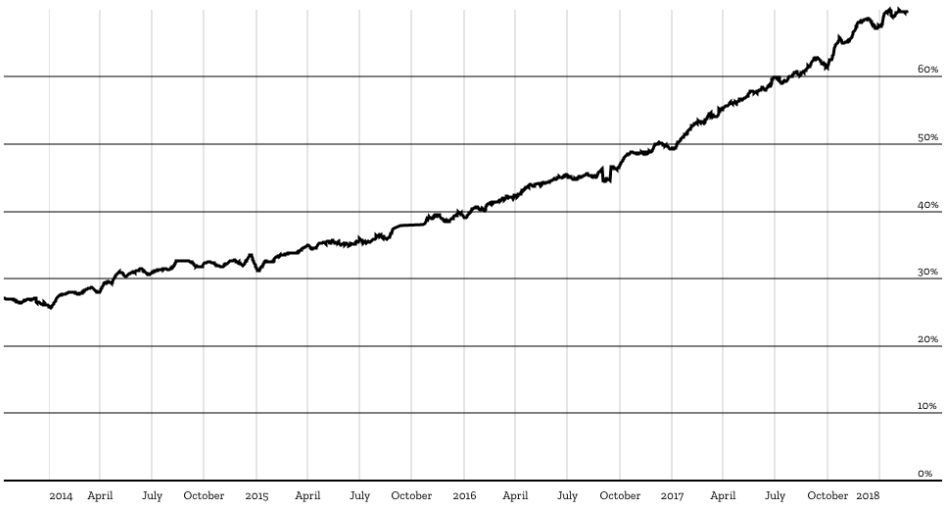
Il s'agit là d'une saine évolution pour Internet.

Le protocole HTTPS protège mieux des pirates les informations que vous saisissez sur un site web, telles que vos données de connexion de messagerie électronique ou celles de vos services bancaires. Aussi, toute personne qui surveille vos activités en ligne peut voir le site web que vous consultez, mais pas les pages spécifiques.

Auparavant, beaucoup moins de sites web utilisaient le chiffrement et l'adoption de cette technologie se faisait lentement. Le déploiement du protocole HTTPS était complexe et exigeait le paiement d'une somme qui pouvait s'élever à plusieurs centaines de dollars par an à une autorité de certification.

Le projet à but non lucratif Let's Encrypt a amélioré la situation en développant des outils ouverts qui facilitent le déploiement gratuit du protocole pour tout site à chiffrer. Ces outils, lancés en décembre 2015, avaient permis, en juin 2017, l'émission de 100 millions de certificats grâce à leur système automatisé.

Pourcentage de pages chargées dans Firefox avec le protocole HTTPS en 2017



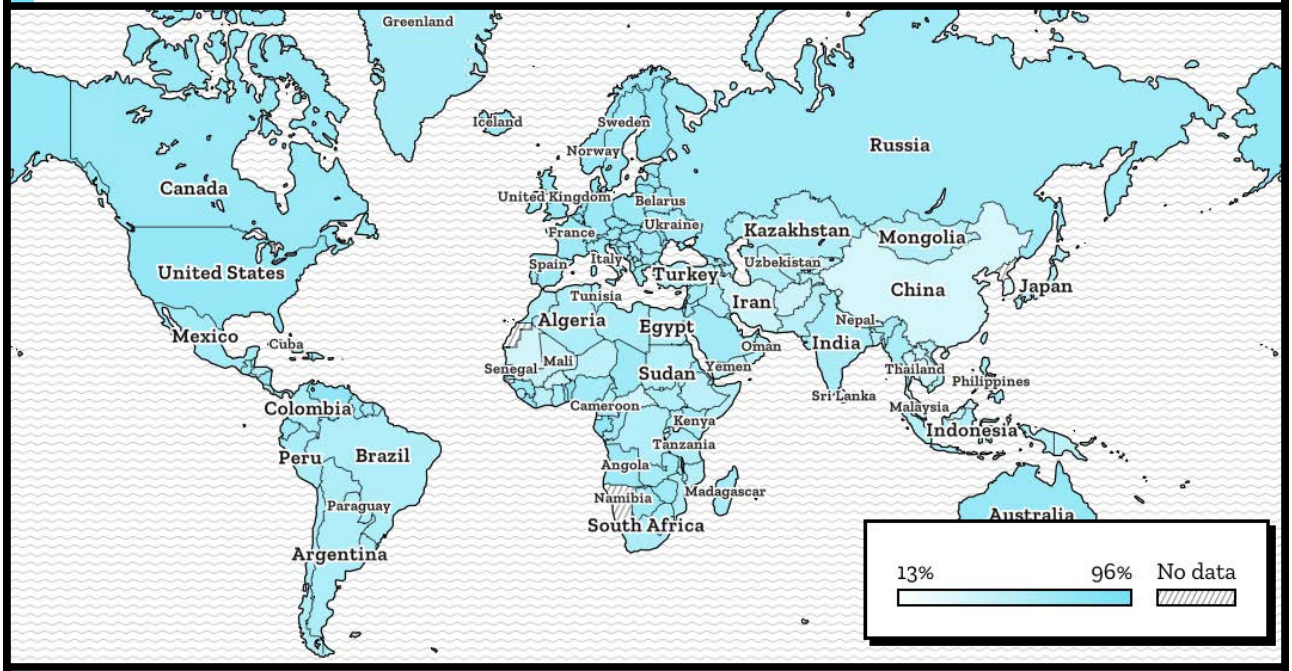
Source des données : Firefox Telemetry, Mozilla 2018

81 des 100 principaux sites web utilisent désormais le protocole HTTPS par défaut. Cependant, selon l'endroit où vous vivez, il est possible que vous accédiez à un nombre beaucoup moins important de sites chiffrés que d'autres personnes ailleurs.

Dans certains pays, les gouvernements peuvent bloquer ou dégrader activement le trafic HTTPS à des fins de surveillance. Dans d'autres cas, les entreprises ou les organisations peuvent manquer de ressources techniques ou de savoir-faire pour mettre en œuvre le HTTPS, ou simplement ne pas le considérer comme une priorité.

Le protocole HTTPS s'étend progressivement à plus de zones géographiques, mais les efforts de sécurisation du Web pour tous encore à déployer restent importants.

Pourcentage de pages chargées avec le protocole HTTPS dans Firefox, par pays



Source des données : Chiffres de télémétrie de Firefox enregistrés du 20 janvier au 20 février 2018. Pour des raisons de confidentialité, les données ne comprennent pas les pays qui comptent moins de 5000 chargements de page.

Vie privée et sécurité // Données

Ce que les sociétés Internet et les fournisseurs d'accès nous cachent

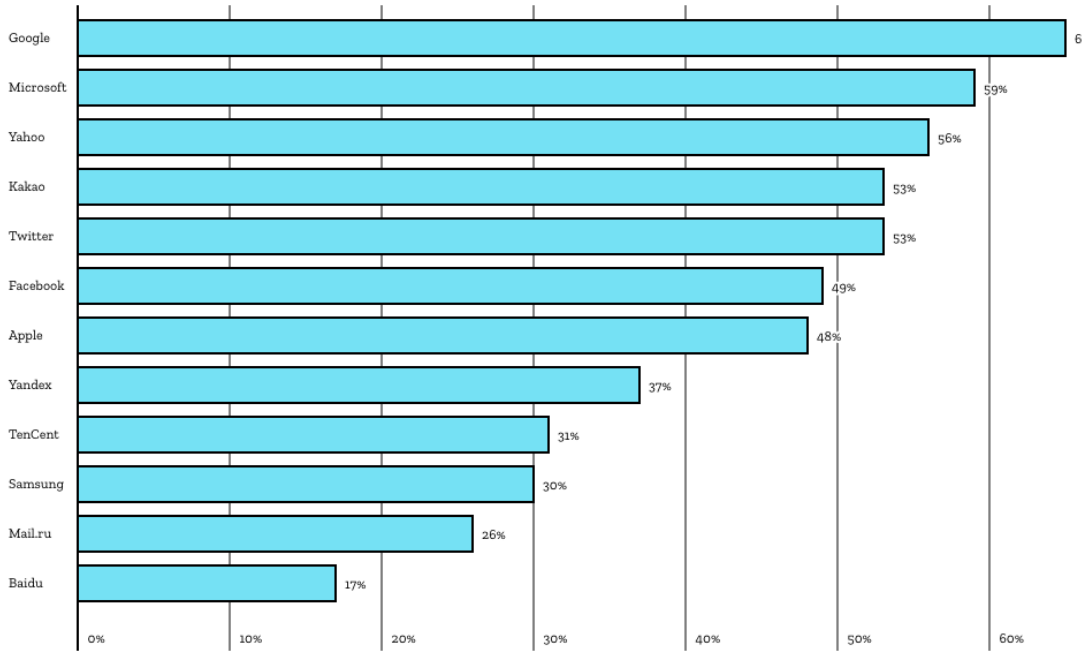
Nous accordons une confiance énorme aux sociétés Internet et aux opérateurs telecom sans recevoir en échange assez d'informations sur leurs politiques de confidentialité et leurs pratiques.

Ranking Digital Rights œuvre à améliorer les normes relatives à la transparence des entreprises sur leurs politiques en matière de gouvernance, de liberté d'expression et de respect de la vie privée au moyen d'un indice de responsabilité des entreprises.

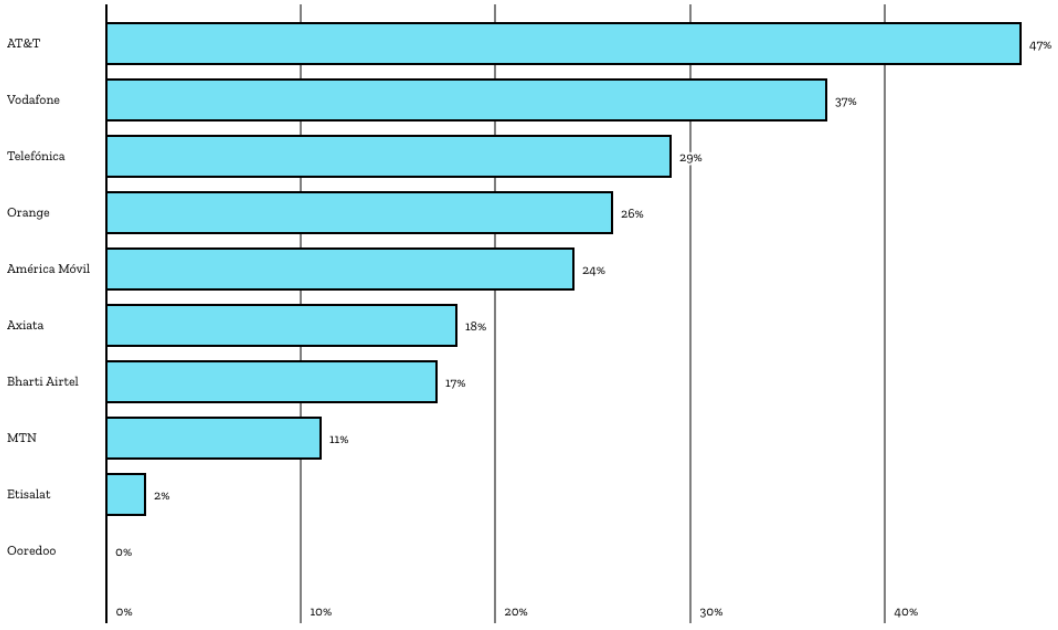
Pour 2017, leurs conclusions sont accablantes : à l'échelle internationale, la plupart des internautes ne disposent pas d'assez d'informations pour faire des choix éclairés. Personne n'en sait assez sur la façon dont nos données sont collectées, partagées, conservées et peut-être réutilisées. De plus, les engagements en matière de gouvernance et de liberté d'expression sont tout aussi insuffisants.

Être en mesure de responsabiliser les entreprises dont nous dépendons pour la connexion et les services Internet nécessite de formuler quels sont nos droits, de comparer les sociétés et d'exiger qu'elles respectent ces droits numériques. Aucune des 22 sociétés qui figurent dans l'indice 2017 n'a obtenu un score supérieur à 65 % en ce qui concerne les mesures de transparence relatives aux droits des clients à la vie privée.

Transparence en matière de politiques et de pratiques relatives à la confidentialité (fournisseurs d'accès Internet et opérateurs mobiles)



Transparence en matière de politiques et de pratiques relatives à la confidentialité (entreprises de télécommunications)



Source des données : Corporate Accountability Index, Ranking Digital Rights, 2017

Vie privée et sécurité // Données

Le top 50 des mots de passe : à améliorer

Les 50 mots de passe les plus communs, tirés des 10 millions d'informations de connexion qui ont fait l'objet de fuites, en disent beaucoup sur notre marge de manœuvre pour améliorer la sécurité sur le Web. Est-ce que vous utilisez « 123456 » comme mot de passe ? Même si ce n'est pas le cas, nous vous conseillons de poursuivre la lecture de cet article.

Un rapport de WP Engine analyse les mots de passe collectés sur le Web à partir de 2015 et partagés à des fins d'études de sécurité. Sur la base de leur fréquence, WP Engine estime que 16 mots de passe sur 1000 pourraient être devinés avec les 10 premiers de cette liste.

L'article Unmasked: What 10 million passwords reveal about the people who choose them décrit la longueur moyenne des mots de passe (8 caractères), leur robustesse moyenne (faible) et démontre que la plupart des internautes utilisent des mots de passe faciles à casser, car les mots, les chiffres ou les habitudes d'utilisation de clavier s'avèrent prévisibles.

Quelqu'un pourrait accéder à votre messagerie électronique ou à d'autres comptes simplement en devinant votre mot de passe. De plus, les pirates peuvent également obtenir des données d'un service que vous utilisez et qui a été victime d'une fuite, découvrir ainsi votre mot de passe et l'essayer dans plusieurs autres services. Si vous utilisez le même mot de passe que des milliers d'autres internautes, vous représentez une cible plus facile pour les attaquants.

Cependant, des solutions existent : l'utilisation d'un gestionnaire de mots de passe, les mots de passe générés automatiquement et l'authentification à deux facteurs peuvent véritablement vous aider à conserver vos données en toute sécurité. Avec des mots de passe uniques et robustes, nous améliorons facilement notre sécurité individuelle et pouvons même protéger les appareils connectés contre les attaques mondiales qui mettent en danger la santé d'Internet.

Les 50 mots de passe les plus utilisés

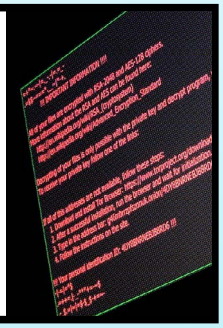
1. 123456	**11.** 123123	**21.** mustang	**31.** 7777777	**41.** harley
2. password	**12.** baseball	**22.** 666666	**32.** f*cky*u	**42.** zxcvbnm
3. 12345678	**13.** abc123	**23.** qwertyuiop	**33.** qazwsx	**43.** asdfgh
4. qwerty	**14.** football	**24.** 123321	**34.** jordan	**44.** buster
5. 123456789	**15.** monkey	**25.** 1234…890	**35.** jennifer	**45.** andrew
6. 12345	**16.** letmein	**26.** p*s*y	**36.** 123qwe	**46.** batman
7. 1234	**17**. shadow	**27.** superman	**37.** 121212	**47.** soccer
8. 111111	**18.** master	**28.** 270	**38.** 121212	**48.** tigger
9. 1234567	**19.** 696969	**29.** 654321	**39.** trustno1	**49.** charlie
10. dragon	**20.** michael	**30.** 1qaz2wsx	**40.** hunter	**50.** robert

Source des données : Unmasked: What 10 million passwords reveal about the people who choose them, WP Engine, 2015

Plus de contenu disponible en ligne

Vie privée et sécurité // Personnes

Histoire d'une victime de rançongiciel



Vie privée et sécurité // Analyse

Les failles de la carte d'identité électronique en Inde devraient tous nous inquiéter

Vie privée et sécurité // Personnes

Découvrez FIRST, les brigades d'urgence de la sécurité informatique

Vie privée et sécurité // Personnes

Nouvelles du front de la lutte contre la surveillance injustifiée

Vie privée et sécurité // Analyse

Le chiffrement en danger dans le monde entier

Vie privée et sécurité // Personnes

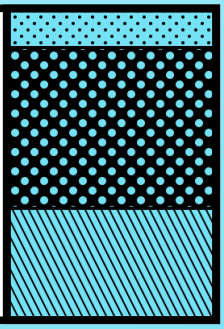
L'expérience-utilisateur au service d'un Internet plus sûr

Vie privée et sécurité // Analyse

Les bons, les mauvais et les horribles côtés du suivi de données

Vie privée et sécurité // Données

Les nerds, plus optimistes à propos de notre futur connecté



Ouvert, jusqu'à quel point ?

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

Nul besoin d'autorisation pour créer de nouvelles technologies destinées au Web. L'ouverture d'Internet permet une innovation constante et une collaboration transfrontalière, de l'architecture du réseau et des logiciels sous-jacents à la publication de contenus en ligne.

Cette ouverture représente un concept radical, constamment menacé.

Les gouvernements bloquent des applications mobiles ou coupent Internet délibérément, les groupes de médias font pression pour obtenir des droits d'auteur étendus dans le monde entier et les entreprises cherchent à verrouiller et à contrôler tout ce qu'elles peuvent : courrier électronique, messagerie, médias sociaux, technologie vocale, réalité virtuelle, apprentissage automatique des machines, etc. pour écraser la concurrence et entraver l'innovation.

Pourtant, l'ouverture d'Internet s'est révélée résiliente et nous avons pu constater des changements positifs en matière de gouvernance et de responsabilisation citoyenne.

En 2017, le débat à ce sujet s'est accentué. Nous avons notamment fait face aux discours haineux, au harcèlement en ligne et à la désinformation dans le monde entier, et les politiques destinées à diviser les citoyens dans de nombreux pays se sont transposées sur les médias sociaux.

Les internautes s'interrogent sur la possibilité de disposer encore d'un Internet à la fois ouvert et inclusif.

Aux États-Unis, ce dilemme a fait les gros titres en août, lorsque des entreprises comme Google, GoDaddy et Cloudflare ont mis fin à leurs contrats de services pour le site web néonazi The Daily Stormer, après un rassemblement nationaliste blanc à Charlottesville, en Virginie. Cette démarche a brièvement rendu le site inaccessible.

L'Allemagne a fait des vagues avec sa « loi sur les discours haineux » controversée, qui a introduit de lourdes amendes pour les entreprises de médias sociaux qui ne supprimeraient pas rapidement des contenus illégaux. Depuis, des pays, y compris la Russie, le Kenya, le Venezuela et les Philippines, ont adopté des réglementations calquées sur le modèle de la loi allemande.

Ces événements traduisent la tension croissante entre la nécessité de contrecarrer la haine en ligne et les risques de placer les entreprises technologiques en arbitres de la liberté d'expression.

Une question urgente se pose aux technologues, aux décideurs politiques et aux citoyens : comment préserver la nature ouverte d'Internet tout en construisant un monde numérique inclusif et accueillant pour tous ?

Ouverture// Données

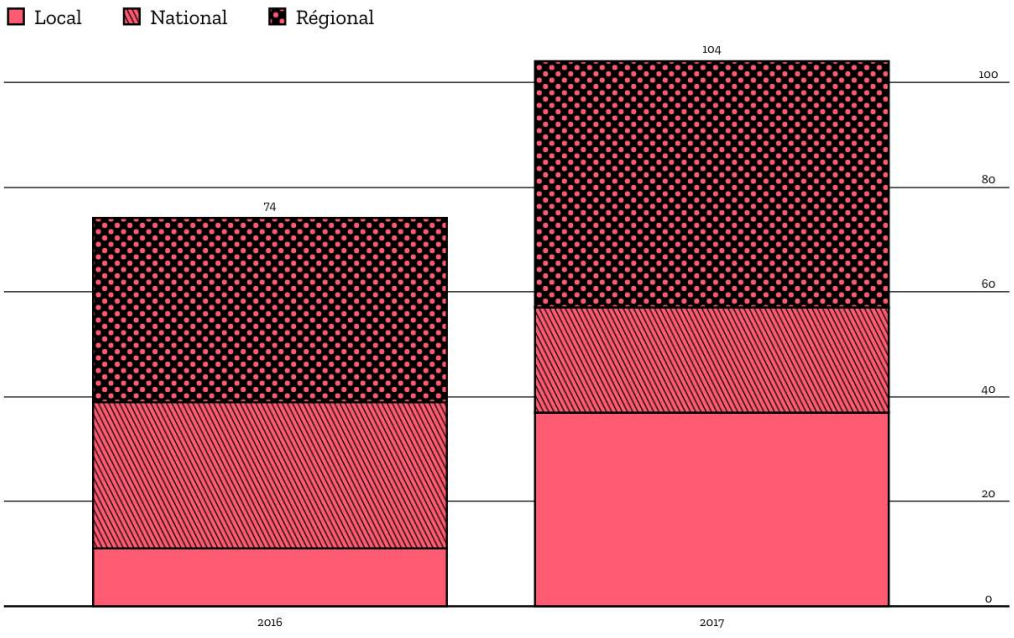
L'explosion des coupures d'Internet

En 2017, le monde a connu au moins 104 blocages d'accès Internet dans 20 pays, certains d'une durée de quelques heures, d'autres de quelques mois, selon l'équipe #KeepItOn d'Access Now qui traque les informations à ce sujet dans le monde entier. Les justifications avancées pour expliquer ces coupures varient, mais un nombre croissant de preuves indique que l'accès à Internet sert d'outil de contrôle et de domination aux autorités de différents pays, par exemple pour faire taire les voix de l'opposition lors de manifestations ou d'élections.

Les cas comptabilisés l'année dernière ciblaient plus souvent les populations locales ou régionales que nationales, ce qui complique la tâche des groupes de la société civile qui luttent pour maintenir un Internet ouvert et tentent de surveiller et de documenter ces événements. Access Now souligne qu'il pourrait s'agir d'une tendance, mais qu'il est difficile de le dire avec certitude. Nous entendons moins d'informations à ce sujet dans les médias, même dans les pays concernés. L'Inde, à elle seule, a autorisé des dizaines de coupures concentrées dans le nord du pays, loin des centres urbains de Bangalore ou de Bombay où de tels blocages ne passeraient jamais inaperçus.

Les coupures maintenues depuis l'année précédente ne sont comptabilisées qu'une fois et ne sont pas comprises dans les chiffres ci-dessous : c'est le cas, notamment, du Pakistan, qui a mis hors ligne des millions de personnes dans une région tribale semi-autonome depuis 2016 ou le nord-ouest et le sud-ouest du Cameroun, qui est resté sans connexion Internet pendant de longues périodes.

Signalements de coupures d'Internet à l'échelle locale, régionale et nationale dans le monde



Source des données : #KeepItOn, Access Now, 2017

Se retrouver sans connexion Internet constitue une situation extrêmement déstabilisante pour les étudiants, les familles et la vie professionnelle. Cela peut devenir traumatisant, voire mortel en période de conflit ou d'attaques terroristes. Les coupures entraînent de graves répercussions sur la sécurité, la liberté d'expression et le réseau lui-même.

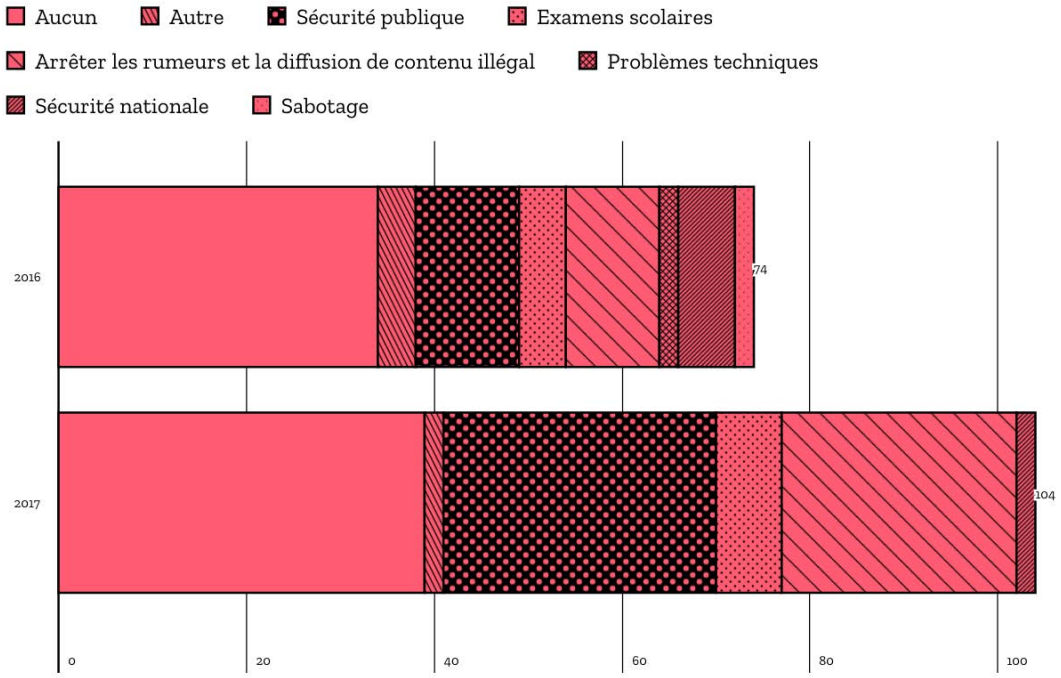
La grande majorité des cas enregistrés l'année dernière ont eu lieu en Asie et en Afrique, et s'accompagnaient de justifications qui vont de l'action « réactive » en réponse à des conflits ou à une activité politique à l'action « préventive » pour stopper une activité indésirable.

L'année dernière, près de 7 % des coupures ont été attribuées à la prévention contre la fraude aux examens scolaires, alors que seulement un peu plus d'un quart des justifications officielles entraient dans la catégorie générale de « sécurité publique ». Sur une note plutôt positive, le nombre de coupures sans justification a diminué.

Parfois, seules les connexions mobiles sont concernées, mais celles-ci représentent souvent le seul accès Internet largement disponible.

Ces blocages sont malsains pour Internet. Nous avons besoin de plus de garanties juridiques pour nous en protéger, à l'échelle nationale et internationale. Avec plus d'études et de collecte de preuves pour déterminer le nombre de coupures et leurs raisons, nous pourrons définir de meilleures tactiques et technologies pour y mettre un terme pour de bon.

Justifications officielles pour les coupures d'Internet dans le monde



Source des données : #KeepItOn, Access Now, 2017

Lieux où les applications de médias sociaux et de messagerie ont été muselées

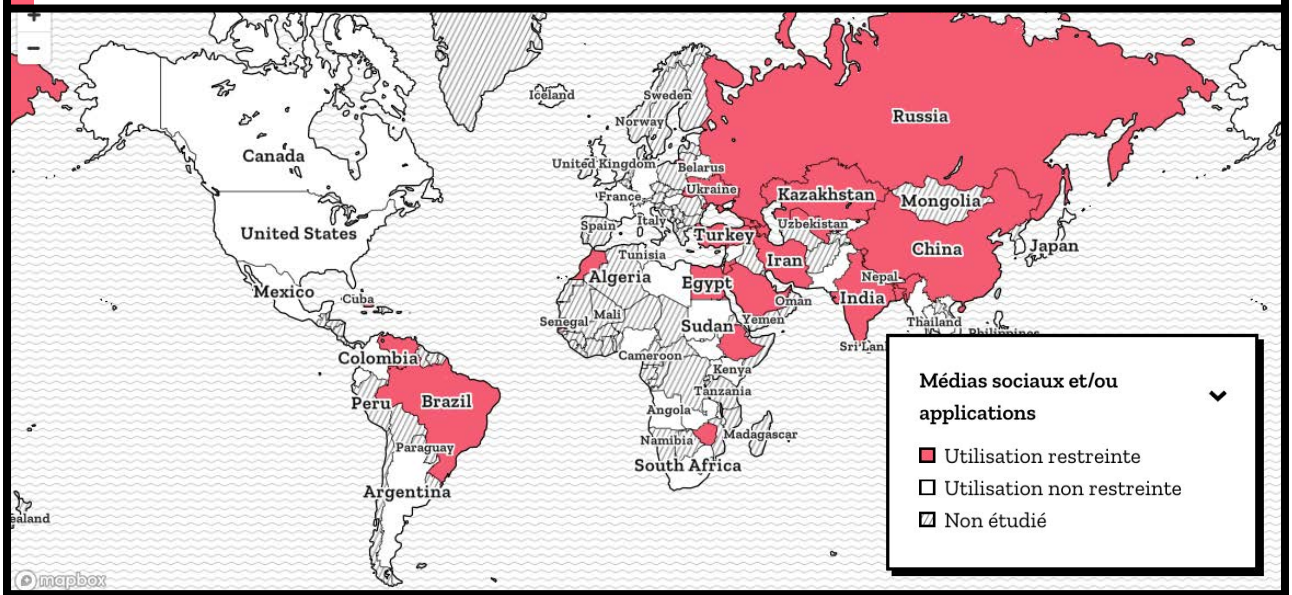
Lorsque les gouvernements souhaitent limiter la liberté d'expression, ils se tournent souvent vers les outils de communication les plus utilisés par les utilisateurs : les médias sociaux en ligne et les applications de messagerie. Partout dans le monde, l'accès à ces technologies est parfois restreint temporairement ou pour de longues périodes selon les caprices des autorités gouvernementales.

La censure sur Internet, les arrestations, les coupures d'Internet et la désinformation font partie d'une panoplie croissante de techniques de répression qui ont toutes contribué à une baisse de la liberté d'Internet sept années consécutives, selon le groupe de défense des droits dans le monde Freedom House.

Selon Freedom House, WhatsApp a été l'application la plus souvent bloquée ou restreinte entre juin 2016 et mai 2017. Ce fut le cas dans 12 des 65 pays analysés par l'organisation. Facebook, Twitter, Skype, YouTube, VKontakte et WeChat figuraient également parmi les services ciblés dans 26 pays différents.

Les deux tiers des internautes vivent dans des pays où la censure d'Internet et des médias est monnaie courante. Lorsque les applications ou les plateformes de médias sociaux sont bloquées, cela empêche l'ensemble de la population (régionale ou nationale) de communiquer avec sa famille, ses amis et ses abonnés. Il s'agit d'une mesure contraignante, qui pourrait avoir de graves conséquences négatives.

Pays où les applications de médias sociaux et de messagerie ont été bloquées



Source des données : Freedom of the Net 2017, Freedom of the Net 2016, Freedom House

Ouverture // Données

Le partage des données ouvertes par les gouvernements stagne

Lorsqu'Internet sert à partager ouvertement des informations publiques, il contribue à améliorer la transparence et la responsabilité du gouvernement et à exploiter son potentiel d'impact positif dans le monde.

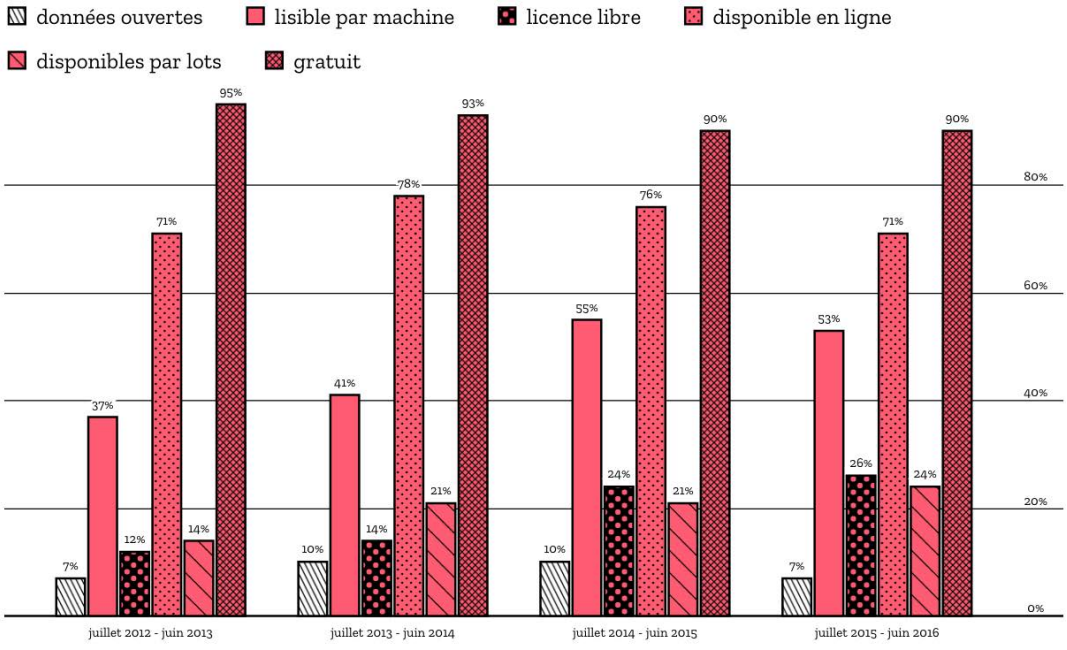
Les données sont considérées « ouvertes » quand elles peuvent être librement utilisées, modifiées et partagées par quiconque et pour tout usage. Idéalement, les données publiques sur les budgets, les élections, les transports, les soins de santé et plus encore, peuvent être consultées en ligne par tous. Malheureusement, les engagements des gouvernements à ouvrir leurs données semblent stagner dans le monde entier.

Les exceptions notables comprennent le Canada, Israël, le Kenya, la Corée du Sud, le Mexique et le Royaume-Uni, qui ont fait des progrès constants depuis l'adoption officielle d'une Charte de données ouvertes.

Le format de publication des données importe énormément pour déterminer si elles possèdent une réelle utilité. Pour servir de manière optimale et bénéficier au public, les données doivent être accessibles en ligne gratuitement, disponibles par lots dans un format lisible par machine (pour leur analyse), et publiées sous licence ouverte (pour offrir la possibilité de réaliser des recherches transsectorielles et davantage).

Le Baromètre des données ouvertes de la World Wide Web Foundation suit les progrès réalisés en matière de données ouvertes dans le monde entier. Sur les 1725 ensembles de données étudiés, dans 115 pays, seulement 7 % étaient véritablement « ouverts » en 2016.

Détails relatifs aux jeux de données publiques partagés par 115 pays entre 2012 et 2016

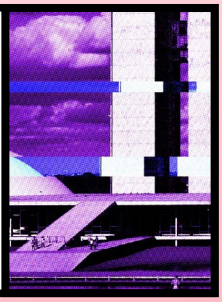


Source des données : Open Data Barometer (4th edition), World Wide Web Foundation, 2017

Plus de contenu disponible en ligne

Ouverture // Personnes

Au Brésil, un bot informatique pour défendre les intérêts publics

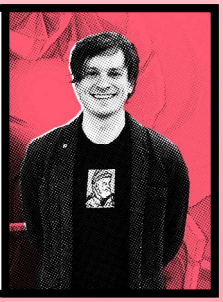


Ouverture // Personnes

Qui sont les individus menacés pour s'être exprimés en ligne ?

Ouverture // Personnes

Pour une technologie vocale à portée de tous



Ouverture // Analyse

La loi allemande contre les discours de haine provoque des vagues à l'international

Ouverture // Personnes

Les coûts cachés d'un Internet ouvert

Ouverture // Personnes

Nouvelle stratégie pour le réseau international de Creative Commons

Ouverture // Analyse

Résister à un blocage de WhatsApp et de Telegram en Afghanistan

Ouverture // Personnes

Les machines intelligentes n'ont pas toujours raison

Ouverture // Analyse

Refusons que les droits d'auteur étranglent Internet en Europe

Ouverture // **Données**

Les logiciels libres que vous utilisez sans le soupçonner

Qui est le bienvenu en ligne ?

Il ne s'agit pas seulement du nombre de personnes qui ont accès à Internet, mais de savoir si celui-ci est sûr et pertinent pour tous.

Environ la moitié de la population mondiale est désormais connectée et cette proportion augmente à une vitesse inimaginable avant l'avènement des téléphones mobiles et des médias sociaux. Pourtant, les fractures numériques tenaces persistent.

Les personnes déjà défavorisées pour différentes raisons, y compris celles à faible revenu, les communautés rurales, les femmes et les minorités, ont tendance à accéder à Internet en dernier. Et lorsque c'est le cas, elles doivent payer des coûts élevés pour un accès de mauvaise qualité.

Sans un accès Internet abordable, fiable et rapide, le développement économique stagne et la population est privée d'accès à l'éducation, à la santé et aux services gouvernementaux, aux contenus de qualité dans sa propre langue ou simplement de conversations avec la famille et les amis.

Face à la fracture numérique, paradoxalement, la déconnexion devient un luxe à l'heure où Internet s'est frayé une place dans tous les aspects de nos vies et nos espaces publics. Et pour de nombreuses communautés marginalisées, le respect de la vie privée n'a jamais été une option en premier lieu.

Un écart se creuse également entre ceux qui se sentent en sécurité en ligne et les autres. Les discours haineux et le harcèlement en ligne constituent un sérieux problème, qui touche davantage les femmes, les jeunes, les communautés LGBTQ+ et les personnes de couleur.

Ce problème est amplifié par la diversité toujours faible au sein de la plupart des entreprises technologiques (et des communautés open source), ce qui se reflète inévitablement dans les logiciels, les algorithmes et les produits développés, qui ne tiennent pas compte des besoins des utilisateurs marginalisés.

Sur tous ces points, nous pourrions dire que la santé d'Internet se dégrade. Cependant, nous avons constaté une série d'efforts nouveaux et significatifs pour favoriser l'inclusion numérique.

En 2017, la forte indignation publique a conduit plusieurs plateformes, dont Facebook et Twitter, à prendre plus au sérieux la lutte contre le harcèlement en ligne. Par ailleurs, nous avons constaté l'émergence de nouvelles initiatives indépendantes pour proposer un accès Internet aux personnes non connectées, étayées par des preuves que les systèmes d'accès de faible qualité destinés aux plus démunis (par exemple le taux zéro) ne représentent pas des rampes d'accès à Internet efficaces. De plus, des études ont révélé des tendances vers la création de communautés en ligne plus inclusives.

L'inclusion numérique apportera de nouveaux défis dans les années à venir. Les fabricants du secteur technologique, les gouvernements et la société civile doivent se rapprocher pour étudier sérieusement ces questions et trouver des solutions à ces problèmes complexes. La possibilité de tirer profit d'un Internet plus sain, fondé sur le respect de l'humanité, repose sur eux.

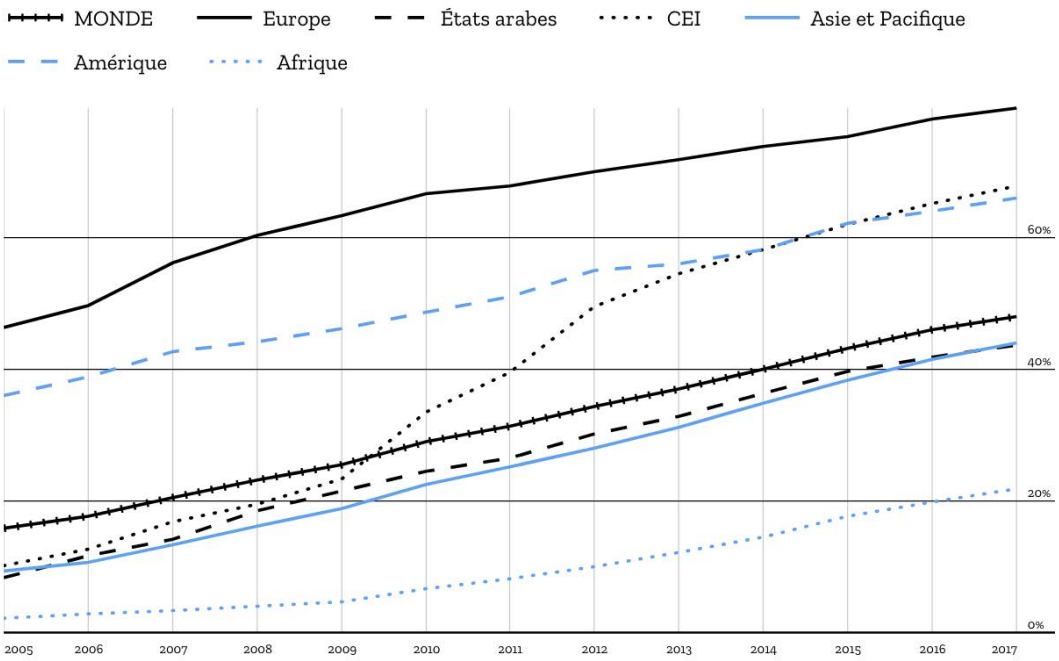
Qui est en ligne ? Qui ne l'est toujours pas ?

Près de la moitié de la population mondiale est désormais connectée, mais le taux de connectivité reste extrêmement inégal d'une région du monde à une autre. En Europe, près de 80 % de la population possède un accès à Internet, alors que ce taux atteint à peine 20 % en Afrique, malgré l'adoption rapide des téléphones portables dans la plupart des pays.

Selon l'Union internationale des télécommunications (UIT), à l'échelle mondiale, l'augmentation n'a été que de 5 % en un an. Comme l'accès à Internet s'avère fondamental pour le développement économique, nous avons un besoin urgent de plus d'abordabilité, d'accessibilité et de qualité pour les populations qui en ont le plus besoin.

L'augmentation actuelle de la connectivité concerne principalement les jeunes internautes : près du quart d'entre eux sont âgés de 15 à 24 ans. Cependant, même dans cette tranche d'âge, il existe des écarts considérables entre régions géographiques. En Europe, 96 % des jeunes disposent d'un accès à Internet, contre seulement 40 % en Afrique.

Augmentation du pourcentage de personnes en ligne dans le monde



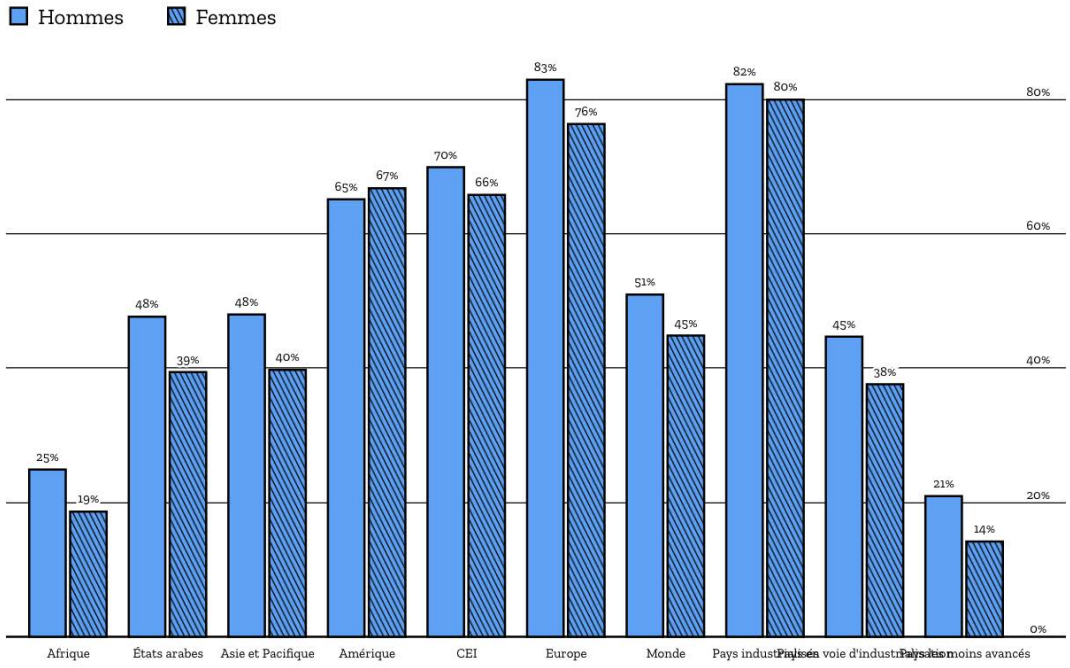
Sources des données : Time series of ICT data for the world, Union internationale des télécommunications (UIT), 2017

Même lorsque le nombre de personnes en ligne augmente, les femmes ne possèdent pas la même probabilité d'en profiter : dans toutes les régions du monde, sauf sur le continent américain, les hommes sont plus nombreux que les femmes en ligne.

Partout où existent des disparités entre les genres en matière d'accès à l'éducation, aux droits sociaux et économiques, les femmes sont moins nombreuses à bénéficier d'un accès à Internet. De fait, la fracture numérique contribue aux inégalités hommes-femmes, car elle réduit les opportunités professionnelles ainsi que l'accès aux canaux d'information et de communication.

En l'absence de politiques visant à inverser cette tendance, les disparités entre genres peuvent facilement s'aggraver. En Afrique, un quart moins de femmes possèdent un accès à Internet, un écart qui s'est considérablement creusé depuis 2013.

Pourcentage de personnes connectées dans le monde, ventilé par sexe



Sources des données : ICT Facts and Figures 2017, Union Internationale des Télécommunications (UIT), 2017

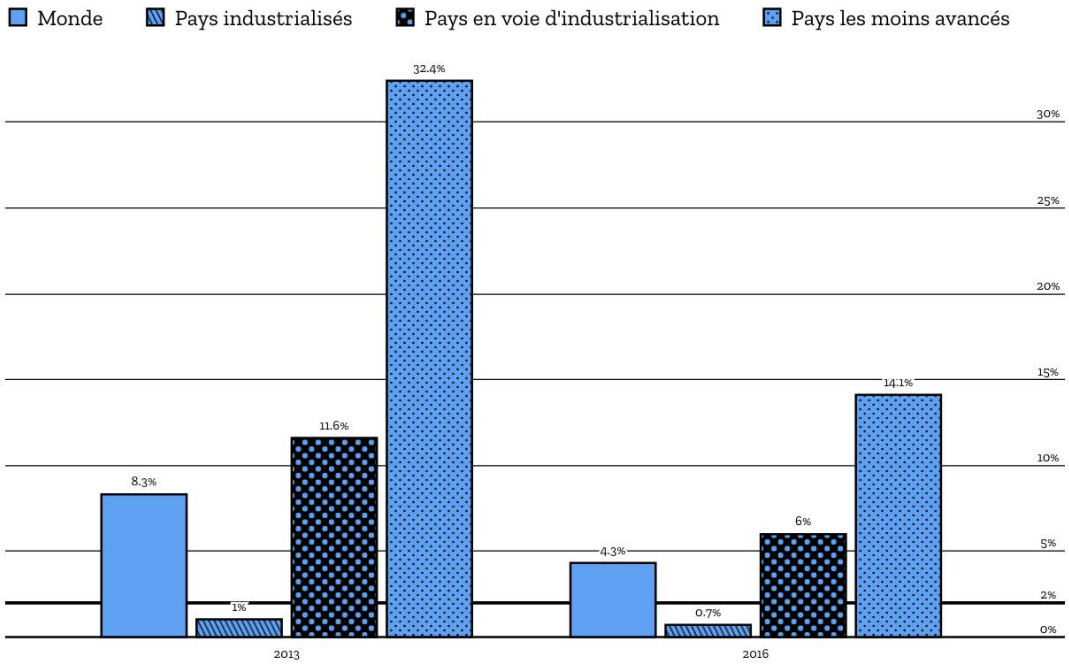
Inclusion numérique // Données

Un accès Internet plus abordable (mais pas encore assez)

Le prix des données mobiles a diminué dans toutes les régions du monde, mais dans les pays les moins avancés, leur coût reste sept fois plus élevé que celui fixé par l'objectif d'accessibilité financière des Nations Unies.

L'accès à Internet est considéré comme abordable lorsque 1 Go de données mobiles haut débit revient à un prix égal ou inférieur à 2 % du revenu national brut mensuel (RNB) par habitant. Réduire le coût de l'accès Internet constitue l'un des facteurs les plus importants pour que le 50 % de la population mondiale qui ne dispose par encore d'une connexion puisse en bénéficier. Cette réduction peut être promue par une série d'interventions politiques, commerciales et techniques. Les groupes de défense d'Internet indiquent que la plupart des pays ne prennent pas suffisamment de mesures concrètes pour atteindre l'objectif de développement durable des Nations Unies qui vise à assurer un accès universel à Internet d'ici 2020.

Prix de 1 Go de données mobiles en pourcentage du revenu national brut mensuel (RNB) par habitant



Source des données : ICT Facts and Figures 2017, Union Internationale des Télécommunications (UIT), 2017

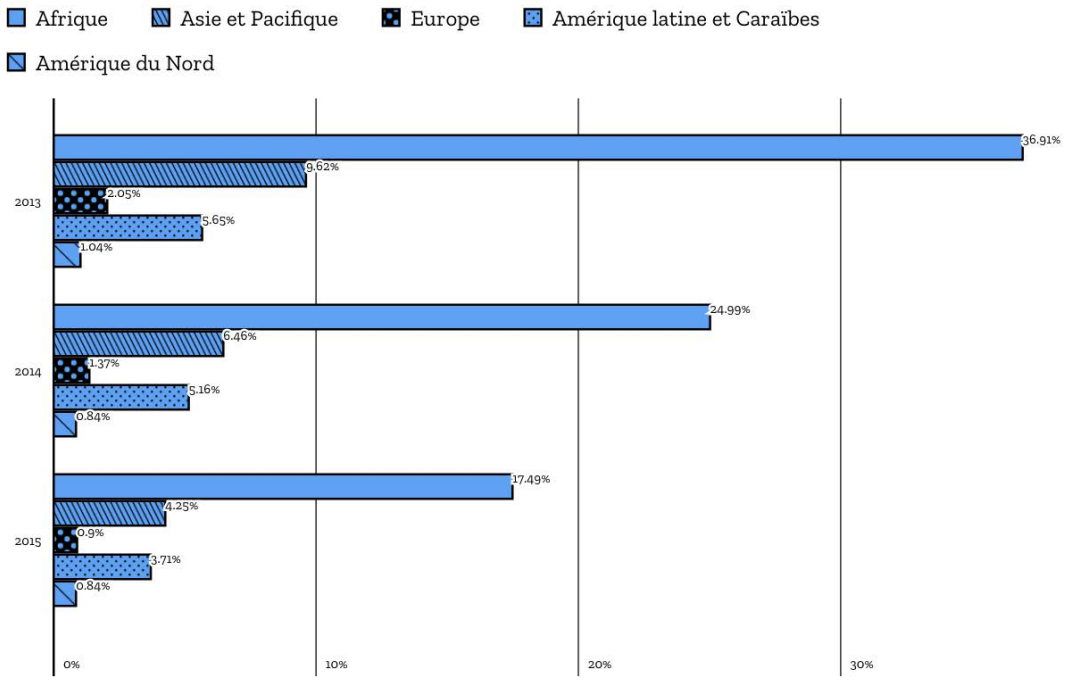
Seules l'Europe et l'Amérique du Nord ont atteint l'objectif d'accessibilité des Nations Unies en 2015. Dans ces régions, les internautes dépensaient moins de 1 % du RNB par habitant pour 1 Go de données mobiles cette année-là.

En Afrique, les gens déboursaient en moyenne 17 % de leur revenu mensuel moyen pour la même quantité de données, et souvent pour des connexions considérablement plus lentes.

L'Alliance for Affordable Internet (A4AI) est l'un des organismes qui a encouragé l'Union Internationale des Télécommunications des Nations Unies (UIT) à continuer d'actualiser sa méthodologie pour refléter l'utilisation actuelle d'Internet. Par exemple, l'étude d'accessibilité de la connexion haut débit de l'A4AI (qui couvre moins de pays) se concentre uniquement sur les offres de données prépayées, ce qui correspond à la façon dont la plupart des personnes dans les pays à revenu faible et intermédiaire se connectent.

Selon l'une ou l'autre méthode d'évaluation, les améliorations les plus évidentes ont eu lieu en Afrique.

Prix de 1 Go de données mobiles en pourcentage du revenu national brut mensuel (RNB) par habitant, par région



Source des données : calculs réalisés par A4AI selon les prix des données publiés par le 2017 A4AI Affordability Report, 2017

Inclusion numérique // Données

Diversité dans le secteur technologique : peut mieux faire

Aujourd'hui, aux États-Unis, les développeurs de logiciels sont majoritairement des hommes blancs. Les preuves montrent que la faible diversité persistante conduit à des logiciels, des algorithmes et des produits qui reflètent les a priori de leurs créateurs. L'année 2017 a été marquée par les scandales de harcèlement sexuel et de discrimination sexuelle, y compris dans les entreprises Internet et les sociétés de capital-risque.

Cela pose problème pour la santé d'Internet.

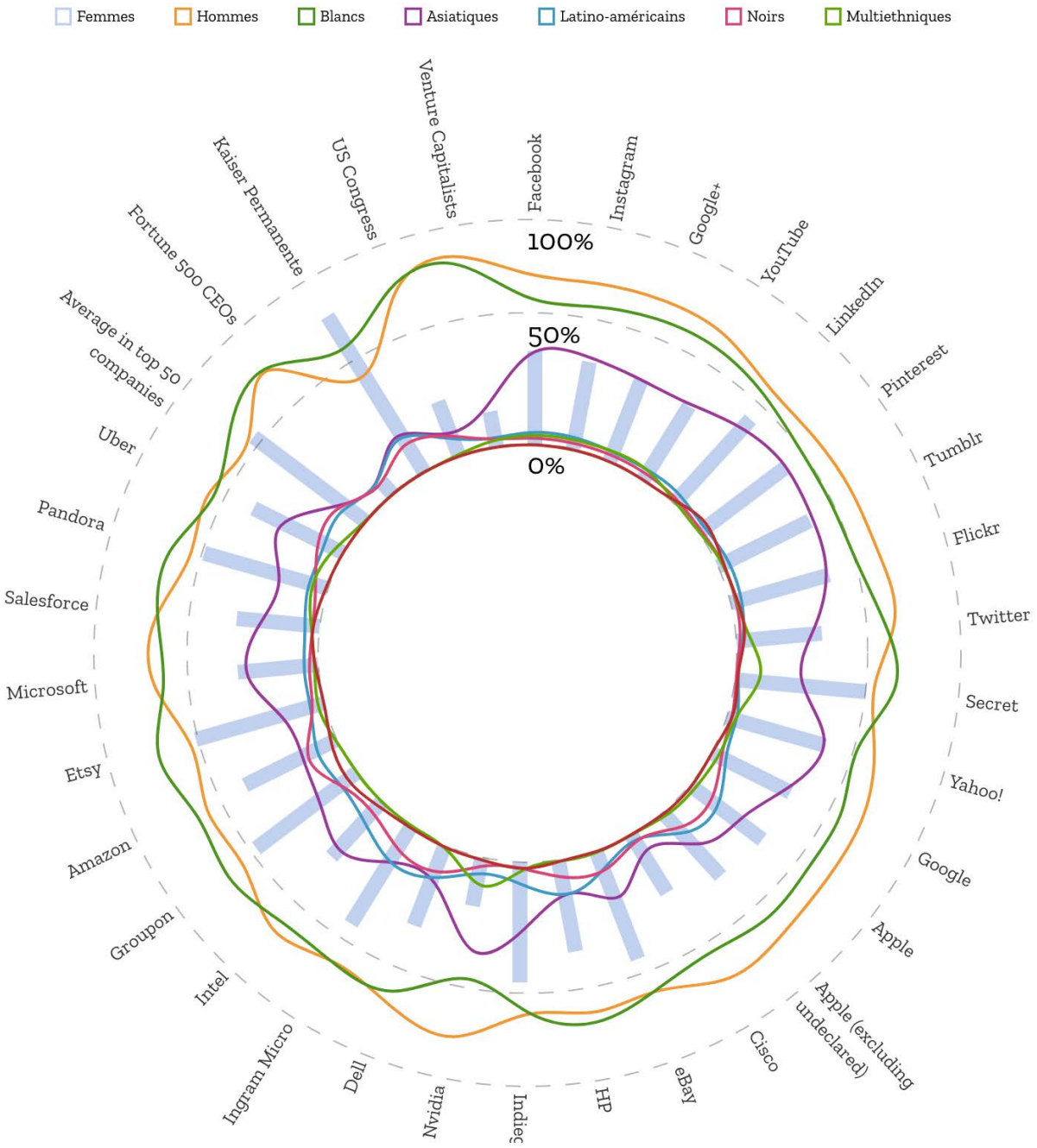
Les attentes pour que les entreprises deviennent plus diversifiées et véritablement inclusives augmentent. Des initiatives comme AnitaB.org, la Société nationale des ingénieurs noirs et Code2040 réduisent les barrières à l'entrée, souvent avec le soutien financier des entreprises elles-mêmes.

Et tandis qu'une plus grande diversité s'avère essentielle, le climat de travail souvent toxique au sein de nombreuses entreprises technologiques devra également changer pour que les membres des communautés sous-représentées aient la possibilité de s'épanouir.

De plus en plus d'entreprises publient les chiffres relatifs à leur diversité et incitent ainsi à une plus grande transparence et responsabilité, mais ces indicateurs ne suffisent pas. Souvent, les progrès en matière de diversité de genre ou ethnique ne se reflètent pas directement sur les équipes d'ingénieurs, ou seulement dans les postes situés au bas de l'échelle salariale.

Reconnaître le problème et gagner en diversité est un bon début, mais pour créer des produits véritablement inclusifs, les entreprises doivent s'appuyer sur un plus large éventail de perspectives, aussi bien du point de vue du genre et de l'origine ethnique que du contexte économique, des langues, des cultures et plus encore.

La diversité ethnique et de genre dans les principales sociétés technologiques des États-Unis



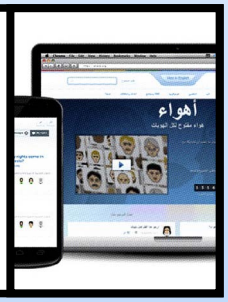
Sources des données : Indicateurs autopubliés relatifs à la diversité dans les sociétés technologiques, selon des données de 2016 ou 2017 compilées dans Diversity in Tech par Information is Beautiful, 2018.

*Les indicateurs de Mozilla relatifs à la diversité pour 2017 seront disponibles durant le deuxième trimestre 2018.

Plus de contenu disponible en ligne

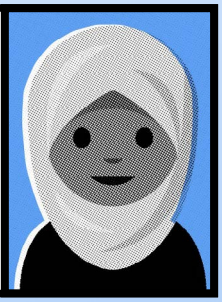
Inclusion numérique // Personnes

Aménager des espaces sûrs en ligne pour les communautés LGBTQ



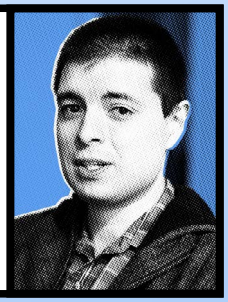
Inclusion numérique // Personnes

Les politiques des émojis pour l'inclusion



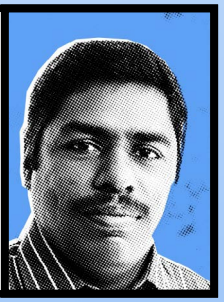
Inclusion numérique // Personnes

Si le problème n'est pas l'anonymat, quel est le problème ? what is?



Inclusion numérique // Personnes

Construire un Internet multilingue



Inclusion numérique // Analyse

De nouvelles approches pour la connectivité des régions rurales

Inclusion numérique // Analyse

Est-ce qu'Internet parle votre langue ?

Inclusion numérique // Personnes

Une permanence téléphonique pour les victimes de « vengeance pornographique »

Inclusion numérique // Analyse

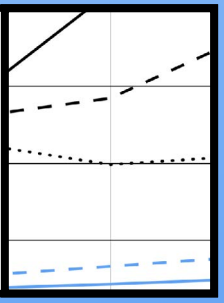
Lutter contre le harcèlement en ligne à l'aide d'intelligences artificielles

Inclusion numérique // Données

Testez vos connaissances au sujet du cyberharcèlement dans le monde

Inclusion numérique // Données

Votre connexion Internet gagne-t-elle en rapidité ?



Vers une égalité des chances ?

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

L'éducation au Web se trouve à notre portée. Nous sommes habitués à nous adapter constamment à de nouveaux logiciels et équipements, autant dans la sphère privée que publique. La conception d'appareils intuitifs permet à des centaines de millions de personnes de prendre en main leur premier smartphone sans se référer à un manuel et, dans certains cas, sans savoir lire.

Cependant les compétences de base que nous développons au fur et à mesure ne nous apportent pas toutes les connaissances nécessaires pour tirer profit des opportunités et éviter les écueils de la vie numérique. Les nouveaux internautes se retrouvent avec une longue liste d'éléments à apprendre, et même les experts ont parfois besoin d' instructions pour faire fonctionner correctement certains services.

Acquérir le large éventail de compétences nécessaires pour lire, écrire et participer à notre monde numérique nécessite une certaine implication. Les connaissances techniques, telles que le codage revêtent de l'importance, mais ne suffisent pas.

Nous devons également être en mesure d'analyser de façon critique les informations que nous rencontrons en ligne, comme l'a rappelé la débâcle des médias sociaux face à la désinformation de l'année passée. Même les jeunes considérés comme des »enfants du numérique » ne savent pas intuitivement quand remettre en question les contenus qu'ils rencontrent ou comment confirmer leur authenticité.

Les plateformes peuvent proposer davantage de transparence quant à l'origine des contenus et soutenir les études qui visent à améliorer la « santé conversationnelle », mais les individus et les communautés doivent également savoir garantir leur propre sécurité en ligne. Cela s'avère particulièrement urgent pour les personnes exposées à la cyberintimidation, au harcèlement ou aux persécutions gouvernementales, mais tout individu peut devenir vulnérable. Si vous utilisez des mots de passe qui figurent parmi les plus couramment employés, les informations relatives à votre vie privée et vos finances se trouvent déjà en danger. Sommes-nous, ainsi que nos enfants, autant en sécurité que possible ?

Sommes-nous capables d'éteindre nos écrans quand cela s'avère nécessaire ? En 2017, les entreprises technologiques ont été la cible de critiques de leur propre secteur pour nous avoir si efficacement rendus dépendants à leurs services. Les applications que nous employons le plus longtemps ne nous rendent pas toujours heureux, et pourtant nous continuons à cliquer et à faire défiler notre écran.

Partout, les internautes doivent posséder toutes ces compétences, et d'autres encore, pour engager des débats plus vastes sur les structures économiques et la dynamique des pouvoirs du Web, qui ont une incidence sur l'ensemble de nos vies. Ainsi, l'éducation universelle au Web s'avère nécessaire. Nous devons soutenir les formateurs et apprendre les uns des autres. Cela devient toujours plus essentiel à mesure que de nouvelles personnes accèdent à Internet, dans le monde entier et au quotidien.

Éducation à Internet // Données

Et si nos applications mobiles nous rendaient malheureux ?

Les applications de nos smartphones peuvent nous causer différentes émotions, pas toujours positives. Le temps que nous passons à tapoter sur nos écrans peut susciter l'anxiété, l'envie, la dépression ou la colère, même Facebook l'admet. Enfin… presque.

L'équipe de Moment (une application iOS gratuite qui enregistre le temps passé à l'écran par les utilisateurs et les aide à limiter l'utilisation d'applications) a réalisé un partenariat avec le Center for Humane Technology, une initiative qui questionne les répercussions de la technologie sur le bien-être et vise à déterminer quelles applications nous rendent le plus heureux ou le plus malheureux.

L'objectif : encourager une plus grande prise de conscience à propos de l'utilisation des applications et provoquer un élan pour changer les mauvaises habitudes.

Dans le cadre de ce projet, Moment a posé à ses milliers d'utilisateurs (pour la plupart situés aux États-Unis et en Europe) une simple question fermée : « Êtes-vous satisfait du temps passé sur cette application ? »

Définir le bonheur n'est pas chose aisée, mais selon les réponses au classement proposé des applications Sonos, Audible, Headspace et Sleep Cycle suscitent de la joie, alors que Facebook, Instagram, Telegram et Reddit provoquent de la tristesse.

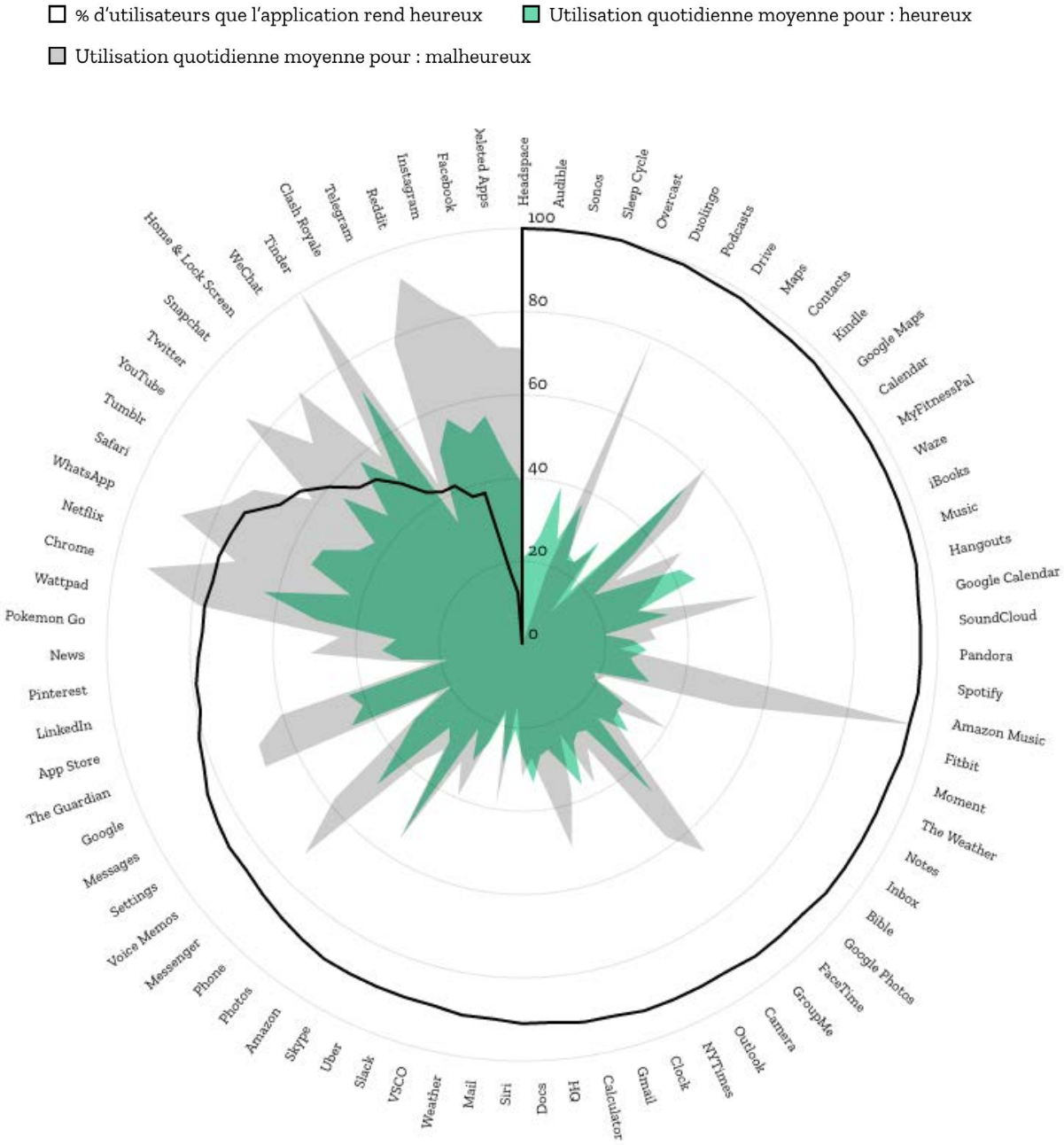
Le temps consacré à une application constitue un élément essentiel. « Je voulais trouver le point de rupture de la satisfaction pour chaque application », explique Kevin Holesh, concepteur de Moment, qui partage régulièrement des informations et des réflexions à propos des statistiques utilisateurs de Moment sur Twitter.

Dans le cas de Facebook, Moment a constaté que ce point se situe à 18 minutes par jour. Un usage modéré de ce type semblerait même mettre les utilisateurs de bonne humeur. Toutefois, lorsque le temps consacré à cette application atteint 47 minutes, celle-ci leur plombe plutôt le moral.

Kevin Holesh souligne que le modèle économique de Facebook repose sur un revenu généré par les interactions avec la plateformes et les revenus des publicités et non sur le « bonheur » que la plateforme procure et doute que Facebook accepte volontiers de réduire les interactions. Si le réseau social souhaitait se positionner sur le marché du bonheur, il devrait réduire les interactions individuelles de 61%, un scénario peu probable.

Alors, si vous sentez votre humeur s'assombrir lorsque vous utilisez votre smartphone, peut-être que vous avez déjà dépassé la dose de moments agréables que votre application préférée est capable de vous offrir. Et si vous avez du mal à la fermer, souvenez-vous qu'il existe désormais une application pour vous aider à le faire.

Les applications qui rendent « heureux » et « malheureux » selon les utilisateurs de Moment



Source des données: Résultats du sondage de l'application Moment partagés par Kevin Holesh, février 2018 (un jeu de données antérieur était disponible sur le site du Center for Humane Technology en 2017)

Éducation à Internet// Données

L'éducation suit-elle l'évolution du Web ?

Seules certaines compétences clés en matière d'éducation au Web sont bien représentées dans les programmes de formation à l'échelle internationale.

Afin de déterminer si les étudiants se trouvent sur la bonne voie pour développer les connaissances nécessaires à l'ère du numérique, Mozilla a étudié huit importants systèmes de formation pour l'éducation et le monde du travail, de façon à définir quelles compétences essentielles en matière d'éducation au Web y figuraient et lesquelles manquaient.

Auparavant, les compétences numériques enseignées se centraient sur l'utilisation des ordinateurs et des logiciels de base. Désormais, les travailleurs, les étudiants et tous les citoyens doivent savoir comment effectuer des recherches en ligne, évaluer les sources (compétences comprises dans tous les systèmes examinés), mais aussi écrire du code de base et comprendre comment naviguer sur le Web (compétences qui y figurent parfois seulement).

Pour profiter d'un Internet en bonne santé, nous devons établir des normes élevées afin que les internautes tirent le meilleur parti de leurs expériences en ligne pour eux-mêmes, leur travail et la société.

Compétences web comprises dans les systèmes de formation pour l'enseignement et le monde du travail

Source des données : Analysis of Mozilla's Web Literacy Map and other Literacy Standards, Mozilla, 2017

Plus de contenu disponible en ligne

Éducation à Internet // Personnes

Un remède à notre culture de la technologie jetable culture

Éducation à Internet// Personnes

Django Girls : de l'Argentine au Zimbabwe, le code informatique

Éducation à Internet // Personnes

Le manuel du Web par excellence, en 48 langues

Éducation à Internet // Analyse

Vos meilleurs conseillers sur le cyberharcèlement ? Les anciennes victimes

Éducation à Internet // Personnes

Enseigner la sécurité numérique à la société civile

Éducation à Internet // Personnes

Un jeu éducatif pour lutter contre la désinformation en ligne

Éducation à Internet// Données

Mobinautes : 53 compétences numériques à acquérir

Qui contrôle Internet ?

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

Internet nous appartient à tous. Il est distribué au moyen d'un réseau décentralisé d'ordinateurs qu'aucune autorité ne peut posséder. Tel est le rêve ; la réalité demeure quelque peu différente.

Hors de la Chine, Internet est dominé par cinq entreprises étasuniennes qui ont développé des technologies utilisées et appréciées par des milliards de personnes. Cependant la consolidation de leur pouvoir et leurs modèles économiques qui exigent de tout savoir sur tout le monde constituent une menace pour la santé d'Internet.

Les sérieuses interrogations visant à déterminer s'il est temps de sanctionner les grandes entreprises du secteur technologique voire de démanteler les grands groupes se font toujours plus urgentes.

En 2017, Google a écopé d'une amende vertigineuse de 2,8 milliards de dollars de la part de la Commission européenne au terme d'une procédure de sept ans. En outre, l'influence démesurée d'une poignée de sociétés de médias sociaux semble encore plus évidente depuis que Facebook, Twitter et Google ont été officiellement rappelés à l'ordre pour l'utilisation de leurs plateformes par la Russie dans le but de diffuser des éléments de désinformation lors de la dernière campagne présidentielle étasunienne.

En Chine, la domination du géant de l'application mobile de messagerie WeChat atteindra un niveau sans précédent si les essais menés sur les comptes des 900 millions d'utilisateurs quotidiens pour la transformer en un système d'identification national sont jugés concluants par le gouvernement chinois.

Les entreprises de télécommunications constituent une menace pour la décentralisation lorsqu'elles proposent des offres sponsorisées relatives à des contenus en ligne spécifiques, par exemple la messagerie ou la musique, qui désavantagent les plus petits acteurs. Pour ceux d'entre nous qui considèrent que tous les contenus devraient bénéficier d'un traitement équitable, ce procédé est inacceptable. En matière de neutralité du Net, quelques batailles ont été gagnées, mais le combat est loin d'être terminé.

Aujourd'hui, une question se trouve au centre des préoccupations : comment rééquilibrer les pouvoirs entre les plus grandes sociétés Internet et les milliards d'entre nous qui utilisent leurs services au quotidien ?

Comment gouverner un monde où une poignée d'entreprises possèdent plus de richesse que de nombreuses nations ? Pouvons-nous distribuer davantage le contrôle des technologies Web, au moyen des technologies de pair à pair, de la chaîne de blocs et de nouveaux principes d'organisation pour les médias sociaux ? Il n'existe pas de solutions miracles, toutefois nous pouvons revendiquer des services ouverts et interopérables, des pratiques commerciales plus éthiques ainsi qu'un marché favorable à la concurrence, à l'innovation et à une diversité de services pour tous.

Décentralisation // Données

Le soutien aux protections de la neutralité du Net progresse

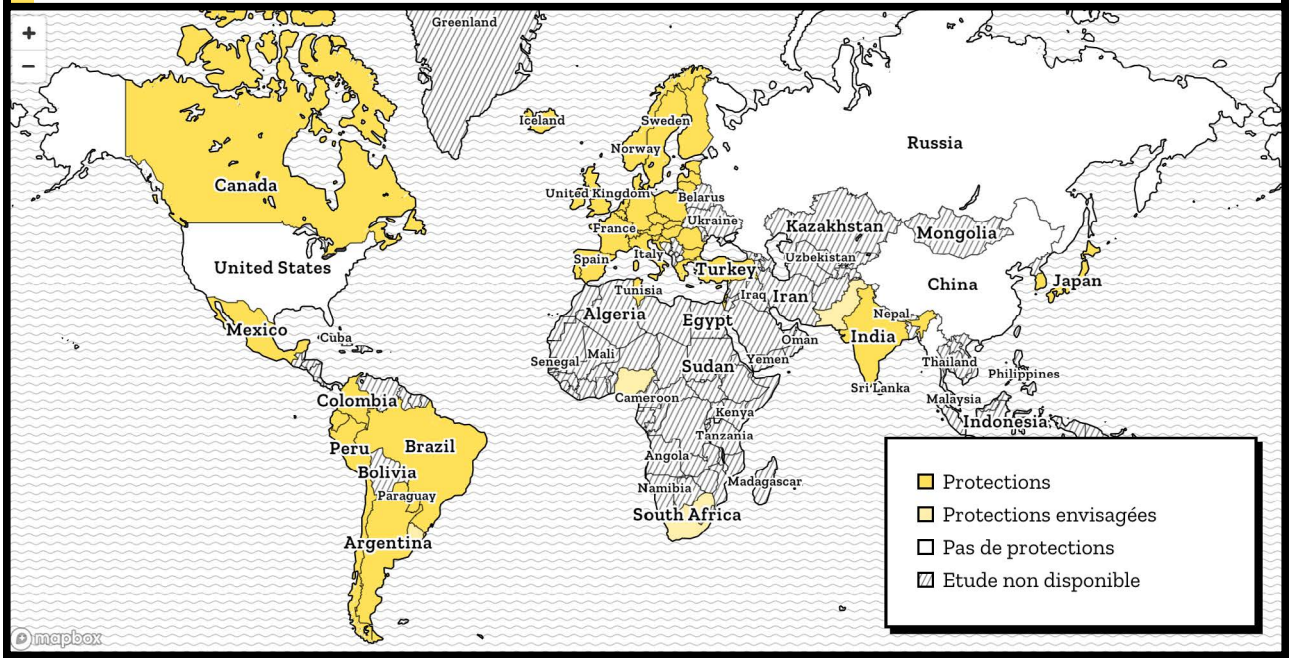
Vous pouvez partir du principe que l'entreprise qui vous connecte à Internet n'a aucun contrôle sur vos activités en ligne, mais peut-être que vous vivez dans un pays où les abonnements Internet restreignent ou favorisent certains contenus musicaux, films ou applications de médias sociaux.

Afin de garantir à tous le même accès au Web ouvert et aux services en ligne que les internautes choisissent d'utiliser, de nombreux pays ont introduit des lois et des protections de la « neutralité du Net ». Lorsque de telles règles sont introduites, c'est souvent parce que les consommateurs s'expriment afin de persuader les régulateurs d'ignorer les puissants lobbyistes de l'industrie des télécommunications.

En 2010, le Chili est devenu le premier pays à inscrire la neutralité du Net dans la loi. Depuis, de nombreux pays ont proposé, adopté ou envisagé de telles protections juridiques pour l'ouverture d'Internet. Malheureusement, certaines victoires sont de courte durée. En 2017, les États-Unis ont abrogé les protections fédérales de neutralité du Net adoptées en 2015. Dans d'autres cas, la loi elle-même ne constitue que le premier pas ; par exemple, la neutralité du Net est entrée en vigueur dans l'Union européenne en 2016, mais la plupart de ses 28 pays membres n'ont pas encore pris de mesures pour faire appliquer cette règlementation.

Malgré les échecs, la sensibilisation du public et le soutien à la neutralité du Net ont augmenté dans de nombreux pays. L'Inde, la deuxième plus grande population en ligne, a renforcé son engagement en faveur de la neutralité du Net en 2017. Certains États américains ont également introduit des protections au mépris des régulateurs fédéraux. Davantage de pays envisagent des protections, y compris l'Afrique du Sud.

État de la neutralité du Net dans le monde



Source des données : Status of Net Neutrality Around the World, Global Net Neutrality Coalition, Access Now, 2017

Décentralisation // Données

Google domine le marché des navigateurs

Google Chrome est le principal navigateur sur les ordinateurs de bureau et les appareils mobiles, et de loin.

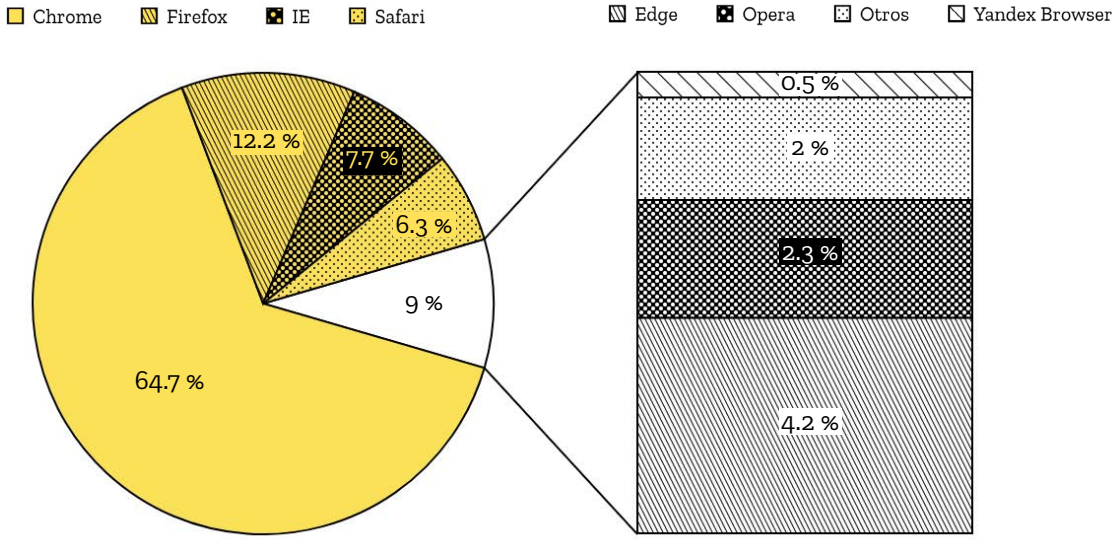
Commercialisé pour la première fois en 2008, Chrome a dépossédé Internet Explorer de Microsoft du titre de navigateur le plus utilisé à un certain point entre 2012 et 2016, selon la méthode de comptage. Depuis, il n'a cessé de progresser, stimulé par l'association avec le système d'exploitation Android.

Sur les ordinateurs de bureau, Firefox (le navigateur soutenu par Mozilla, organisme à but non lucratif) occupe la deuxième place à l'échelle internationale et sur les appareils mobiles, Safari d'Apple et UC Browser d'Alibaba se placent respectivement en deuxième et troisième position.

La principale source de revenus de Google provient de l'affichage et de la vente de publicités. Son navigateur gratuit, Chrome, contribue à cette activité. Toutefois, il existe des effets moins connus de la domination de Google, comme le fait que l'entreprise possède le pouvoir de définir et de mettre en œuvre des fonctionnalités qui façonnent le fonctionnement du Web pour tous, au-delà du navigateur utilisé, par exemple à travers des processus de normalisation du Web. Il s'agit là d'un vecteur de concurrence déplorable, car Google a la possibilité de faire pression en faveur de normes ou de formats que les autres navigateurs ne peuvent pas ou ne veulent pas proposer.

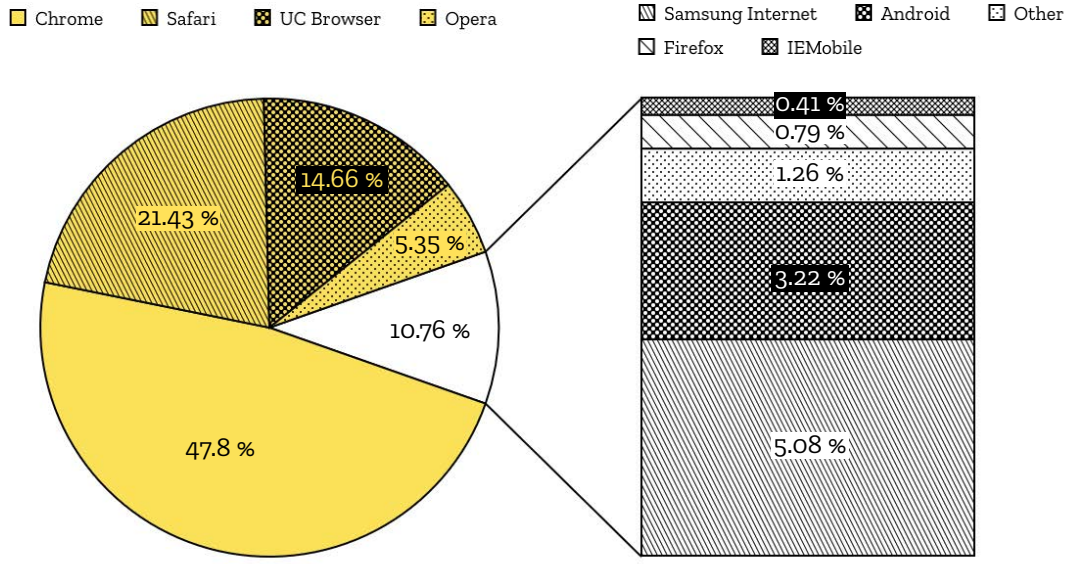
Le navigateur constitue la porte d'entrée vers le Web, de sorte que la concurrence et les options au sujet de valeurs telles que le choix, la confidentialité et la transparence représentent des composantes essentielles pour la santé d'Internet.

Part de marché mondiale du navigateur pour ordinateurs



Source des données : Desktop Browser Market Share Worldwide, StatCounter, 2017

Part de marché mondiale du navigateur pour appareils mobiles



Source des données : Mobile Browser Market Share Worldwide, StatCounter, 2017

Décentralisation // Données

Facebook, Tencent, Google : le règne des géants des médias sociaux

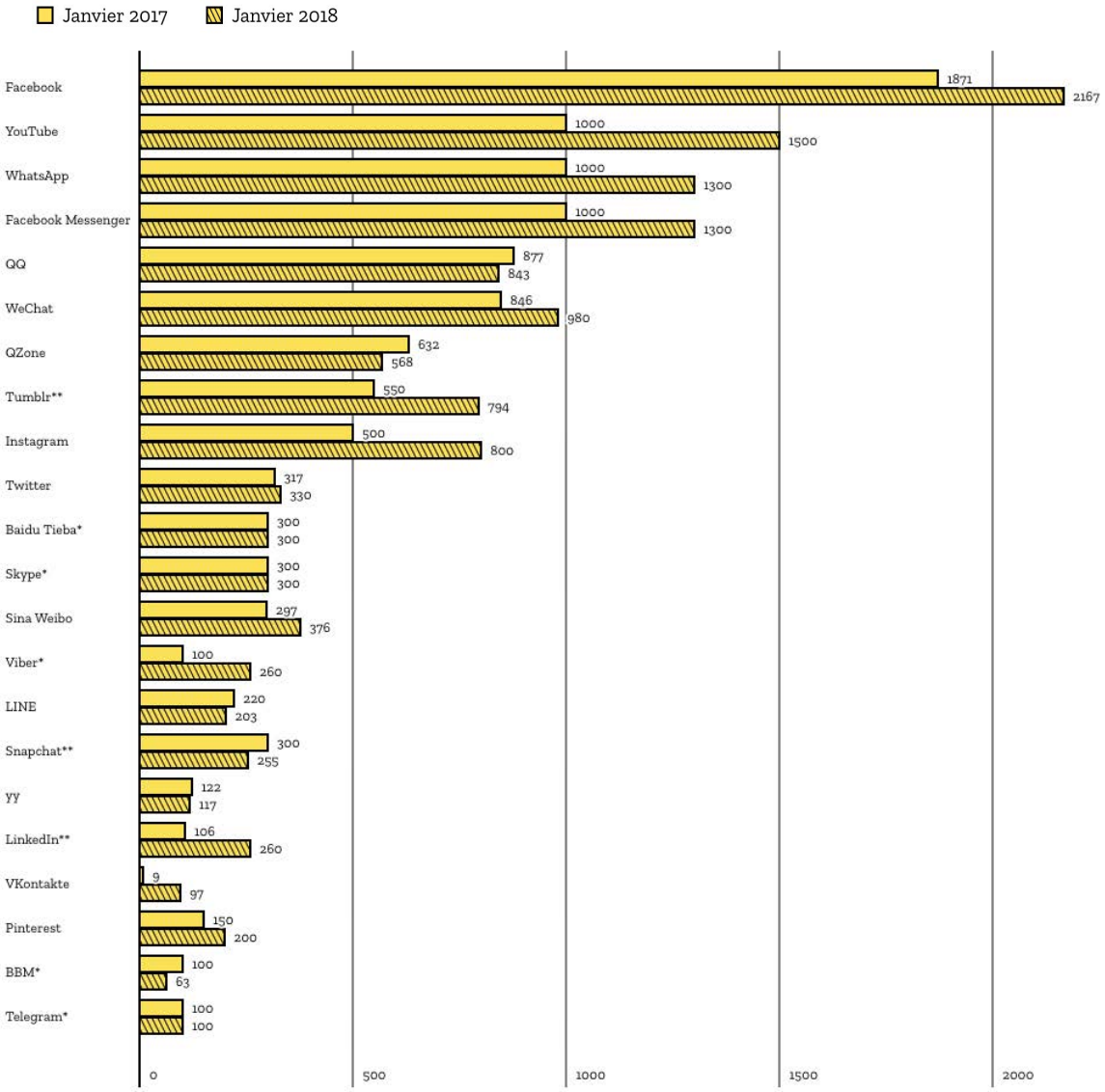
La majorité des 3,57 milliards d'internautes que compte la planète possèdent un compte sur une ou plusieurs des principales plateformes de médias sociaux. À elle seule, Facebook comptait 2,16 milliards d'utilisateurs mensuels actifs fin 2017 et reste le leader incontesté des médias sociaux en matière de rayon d'action et de rentabilité.

Les médias sociaux, accessibles par le Web ou les applications mobiles, sont employés pour échanger des messages et publier des contenus. Toutefois, leur définition devient floue.

Outre être un service de messagerie privée, WhatsApp fait aussi office de plateforme commerciale et d'information. WeChat, la plus grande plateforme de Chine, offre à ses utilisateurs la possibilité de réaliser en son sein pratiquement tout ce que les internautes effectuent en ligne, y compris des achats, le recours aux services bancaires et la navigation sur le Web.

Lorsqu'une poignée d'entreprises contrôlent les communications privées et les données personnelles, ainsi que les photos et les vidéos de milliards de personnes, elles exercent un pouvoir énorme sur les marchés, notre expérience du Web ouvert (ou de son manque d'ouverture), le discours public mondial, la liberté d'expression et notre vie personnelle. La façon dont nous leur demandons de rendre des comptes, et la disponibilité des informations nécessaires pour le faire, représente un élément crucial pour la santé d'Internet.

Utilisateurs actifs des réseaux de médias sociaux les plus populaires dans le monde

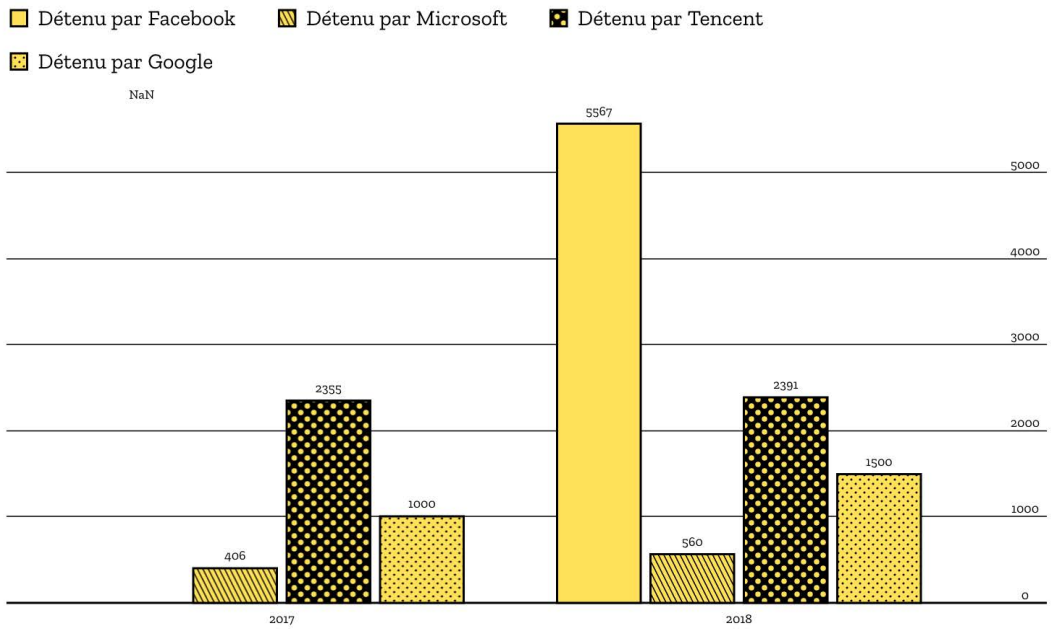


Source des données : Utilisateurs mensuels actifs des réseaux sociaux les plus populaires, Statista, janvier 2018

*Les plateformes n'ont pas publié de chiffres mis à jour au cours des 12 derniers mois. Il se peut que les données soient obsolètes ou moins fiables. **Ces plateformes ne publient pas de données relatives à leurs utilisateurs mensuels actifs, les chiffres proviennent de rapports de tierces parties.

Trois entreprises dominent toutes les autres en termes d'utilisateurs actifs mensuels combinés de tous les services qu'elles possèdent. **Facebook** détient WhatsApp, Facebook Messenger et Instagram. **Google** possède YouTube et **Tencent** possède QQ, WeChat et QZone. Facebook se positionne largement en tête, puisque l'entreprise a dénombré 1,196 milliard de nouveaux utilisateurs sur ses différentes plateformes en un an seulement.

Les réseaux de médias sociaux Facebook, Tencent et Google comptent le plusd'utilisateurs mensuels actifs



Utilisateurs actifs mensuels (en millions)

Source des données : Utilisateurs mensuels actifs des réseaux sociaux les plus populaires, Statista, janvier 2018

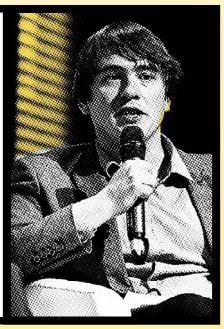
Plus de contenu disponible en ligne

Décentralisation // Données

Moteurs de recherche : plus de 90 % du monde utilise Google

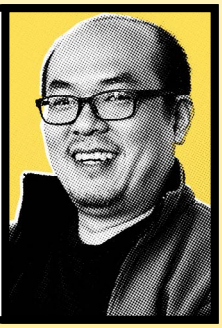
Décentralisation // Personnes

Un observatoire pour la neutralité du Net en Europe



Décentralisation // Personnes

Construire ensemble des drones sous-marins en Chine

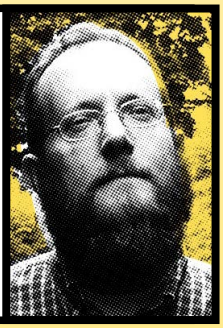


Décentralisation // Personnes

La résistance contre le colonialisme numérique

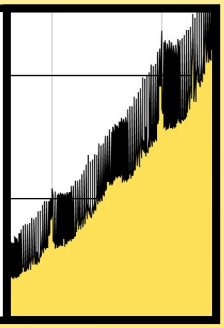
Décentralisation // Personnes

Logiciels recherchent chasseurs de bogues + ("Blockchain")?;



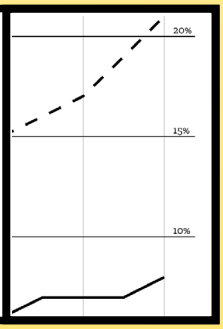
Décentralisation // Données

IPv6, une mise à niveau tardive pour Internet



Décentralisation // Données

Internet utilise plus d'électricité que...



Décentralisation // Personnes

Casper Klynge, premier ambassadeur d'un pays auprès des entreprises technologiques

Participer

Comment agir ?

Après avoir lu ce rapport, il est probable que vous vous posiez la même question que la plupart d'entre nous : que puis-je faire ?

Vous êtes peut-être préoccupé par un problème spécifique, comme la propagation de la désinformation en ligne, la vie privée de votre famille, ou alors votre connexion Internet a possiblement été coupée.

Peut-être que vous êtes déjà activement impliqué dans l'amélioration de la santé d'Internet, par exemple en tant qu'avocat, éducateur, décideur politique, journaliste, chercheur, etc.

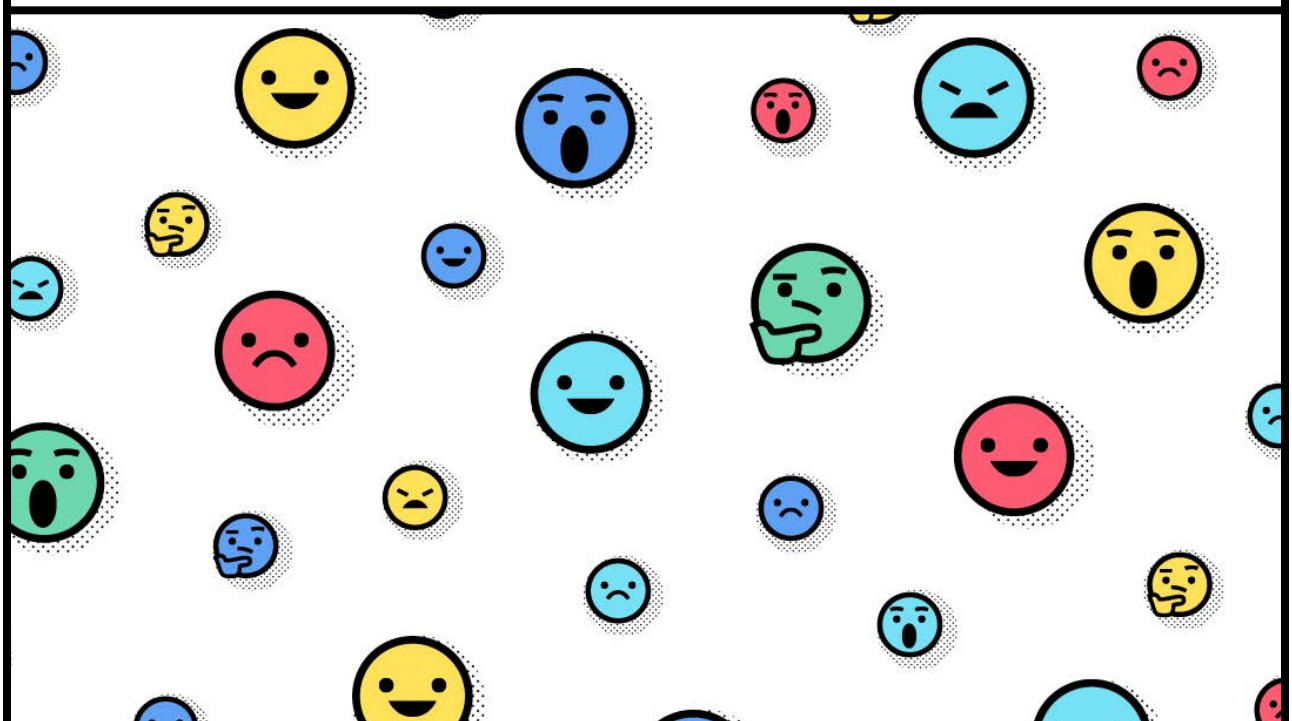
Il est également possible que vous souhaitiez simplement mieux comprendre les technologies qui affectent votre vie et votre communauté ainsi que les possibilités d'organiser ces interactions.

Le Bulletin de santé d'Internet représente le check up d'Internet en ce moment. Il résulte d'un effort collaboratif et représentatif d'un large éventail d'opinions de spécialistes du domaine. Il ne livre pas toutes les réponses et nous pouvons aller jusqu'à dire qu'il multiplie les questions.

Mais il constitue également un appel à l'action. En effet, le défi pour chacun d'entre nous consiste à apprendre et à agir davantage, à travailler ensemble pour créer un Internet sain qui valorise les gens par-dessus tout.

Dans cet esprit, voici quelques réflexions sur la façon de relever ce défi.

- Adopter les bonnes pratiques
- Discuter et débattre
- Retrousser ses manches



Adopter les bonnes pratiques

Utilisez Internet plus sainement et améliorez également l'ensemble de l'écosystème. Vous pourriez commencer par :

- Vous protéger et sécuriser vos appareils à l'aide de mots de passe forts et de l'authentification à deux facteurs,
- Maintenir le système d'exploitation de votre ordinateur et de votre smartphone, ainsi que vos logiciels à jour dès qu'une mise à jour de sécurité est disponible pour vous protéger et protéger vos proches,
- Apprendre à identifier les abus en ligne et connaître vos droits pour réagir si vous ou une de vos connaissances est victime de harcèlement en ligne. Vous avez aussi la possibilité de soutenir ou faire du bénévolat au sein d'organisations qui apportent leur aide aux victimes.
- Explorer quels types de données les sociétés telles que Google ou Facebook collectent à votre sujet et définir des paramètres de confidentialité appropriés pour vous. Et, pourquoi pas, suivre un régime détox en matière de données ?
- Améliorer vos compétences en « détection de bêtises » et essayer de vérifier les photos et vidéos avant de les partager. Renseignez-vous sur les incitations économiques derrière certains contenus de désinformation.
- Vous assurer que le site web que vous possédez ou administrez est accessible uniquement via https (crypté). Si ce n'est pas le cas, contactez votre hébergeur.
- Aider à soutenir la technologie vocale gratuite et ouverte en faisant don de vos enregistrements vocaux au projet Common Voice pour enseigner aux machines comment les gens parlent réellement.
- Identifier les logiciels à code source ouvert que vous utilisez régulièrement et soutenez-les par du temps, de l'argent ou des remerciements. Par exemple, vous pouvez éditer des articles sur Wikipédia, des documents MDN Web ou réviser du code.

Discuter et débattre

Pour améliorer la santé d'Internet, nous avons besoin qu'un plus grand nombre de personnes comprennent les enjeux, s'en préoccupent et agissent.

Nous espérons que ce rapport pourra vous aider à entamer des conversations avec d'autres sur la façon de construire un Internet plus sain, ensemble.

Nous vous invitons **à copier, réutiliser, télécharger et partager ce rapport**, **mais aussi à en débattre et à écrire à son sujet.** Nous avons choisi de le publier sous licence Creative Commons-Attribution (CC BY 4.0) pour en encourager la réutilisation.

Voici trois possibilités pour vous lancer :

Discutez des articles du rapport. Le changement commence par l'action et les actions par des réactions. Après avoir lu un article, choisissez un emoji pour exprimer votre sentiment à propos de celui-ci.

Ensuite, consultez les commentaires pour découvrir les avis des lecteurs et ajoutez votre point de vue. Ce faisant, veillez à respecter nos Directives relatives à la participation communautaire.

Partagez vos articles préférés. Choisissez un sujet ou un graphique qui vous a interpellé et envoyez-le à vos amis ou publiez-le sur les réseaux sociaux. Il vous suffit d'utiliser les boutons « Partager » disponibles au bas de chaque page.

Lancez la conversation dans votre communauté. Nous avons développé de nombreuses ressources pour vous faciliter la tâche, y compris une présentation et un guide pour l'organisation d'événements.

Retrousser ses manches

Il n'appartient pas qu'à vous de faire la différence. Internet deviendra beaucoup plus sain grâce à des changements structurels, à une gouvernance réfléchie et à une meilleure protection des consommateurs de produits et de services partout dans le monde. Vous pouvez continuer à exiger que cela devienne réalité et à vous engager dans des efforts collectifs pour que ces changements se produisent.

Collaborez avec Mozilla

- Découvrez les initiatives et les campagnes politiques de Mozilla
- Envoyez votre candidature pour rejoindre l'équipe des Mozilla Fellows
- Devenez un Mozilla Open Leader
- Participez au Mozfest ou au Global Sprint
- Découvrez d'autres possibilités pour aiderà maintenir Internet en bonne santé

Impliquez-vous directement

Si vous souhaitez vous impliquer pour résoudre un problème spécifique ou si vous vous interrogez sur la santé d'Internet dans votre région du monde ou votre pays, nous vous encourageons à prendre contact avec des groupes locaux de défense des droits numériques. Observez qui s'exprime sur ces sujets et contactez ces personnes.

Les organismes et les individus mentionnés dans ce rapport constituent un bon point de départ.

Nous contacter

L'équipe du Bulletin de santé d'Internet, une publication à code source ouvert, apprécie les commentaires constructifs. Nous encourageons vivement les suggestions au sujet d'études ou de données à inclure dans la prochaine édition. Nous sommes également intéressés par vos réponses aux questions suivantes : Que pensez-vous de cette initiative ? Ce rapport a-t-il changé votre perception d'Internet, suscité des idées de recherche ou vous a-t-il motivé de quelque façon que ce soit ?

Laissez-nous un commentaire public en ligne ou faites-nous parvenir un courrier électronique privé à l'adresse suivante : internethealth@mozillafoundation.org

Pour obtenir les informations les plus récentes au sujet des nos activités, consultez le blog du projet.