Geneva Internet Platform
DigitalWatch
dig.watch

Numéro 45, nov / déc 2019
Newsletter

Berlin 2019: L'aube d'un nouveau FGI ?

TENDANCES

Les discussions sur les questions cyber continuent à l'ONU ; les entreprises de l'Internet prennent de nouvelles mesures pour lutter contre la désinformation et les deepfakes.

Plus en pages 2–3

OBSERVATOIRE

La sécurité, l'économie de l'Internet, les droits numériques, et l'infrastructure ont été des questions à l'agenda au cours des deux derniers mois.

Plus en pages 4–5

ANALYSE DE DONNEES

Nous faisons un état des lieux des fuites de données au cours de cette année : quel en a été le nombre, et quels secteurs ont été les plus affectés ?

Plus en pages 8–9

POUR LE FUN

Tandis que se termine une année chargée pour les politiques numériques, nous vous proposons une version améliorée de la chanson *It's the end of the year and we know it (and we'll be fine)* ...

Plus en page 12

ORGANISATION INTERNATIONALE DE la francophonie

La version française de la newsletter *Digital Watch* a été publiée avec le soutien de l'Organisation internationale de la Francophonie www.francophonie.org

Les principales tendances des politiques numériques en novembre et décembre

Chaque mois, nous analysons des centaines de développements pour identifier des tendances de politiques numériques, et les tendances à venir. Voici les principales tendances des mois de novembre et de décembre.

1. Les discussions sur les questions cyber se poursuivent à l'ONU

Au cours des mois de novembre et de décembre, les Etats membres de l'ONU ont accéléré leurs discussions sur les questions liées à la cybercriminalité et la sécurité des informations. Le Troisième comité de l'Assemblée générale de l'ONU (AGNU) a adopté une résolution pour lutter contre l'utilisation des TIC à des fins criminelles. Proposée par la Russie et 26 autres Etats, cette résolution appelle à l'établissement d'un groupe d'experts ouvert, ad hoc et intergouvernemental, de toutes les régions du monde, visant à développer une convention internationale pour lutter contre la cybercriminalité.

Si cette résolution était adoptée par l'AGNU, ce nouveau comité fondera probablement ses travaux sur un projet de convention proposée par la Russie en 2017 sur la coopération en matière de cybercriminalité. Ce document liste différents crimes (notamment le hacking), présente des options pour améliorer la coopération internationale et propose un centre de contact et de soutien pour mener des enquêtes.

Dans une lettre ouverte à l'AGNU, 36 groupes de défense des droits de l'homme ont mis en garde contre ce projet de convention, estimant qu'elle pourrait limiter la capacité de l'Internet à permettre l'exercice des droits de l'homme. Cette convention donnerait aux gouvernements le pouvoir de bloquer des sites Internet et services en ligne pour des raisons politiques. Ils ont donc invité les Etats membres à s'opposer à cette résolution durant l'assemblée générale.

Une autre question se pose également : quelle serait la relation de cette nouvelle convention onusienne sur la cybercriminalité avec la convention de Budapest, adoptée par le Conseil de l'Europe et ratifiée par plus de 60 pays ? Quelles seraient les conséquences si la cybercriminalité devenait l'objet de deux cadres légaux au niveau international ?

En matière de sécurité des informations, des consultations informelles se sont tenues au sein des groupes de travail sur les développements dans le domaine des télécommunications et de l'information dans le contexte de la sécurité internationale. Les agendas du groupe de travail ouvert (GTO) et du Groupe d'experts gouvernementaux (GEG) étaient très similaires : le paysage des cyber-menaces; les normes, règles et principes du comportement responsable des Etats dans le cyberespace ; les mesures de renforcement de la confiance et de capacités.

Leurs discussions étaient remarquablement similaires également : les activités de phishing, les technologies autonomes, et l'utilisation par les terroristes de la propagande étaient au centre des échanges de ces deux groupes. Chacun a souligné l'importance de la mise en œuvre de normes déjà définies lors de précédents rapports du GEG. Sur le renforcement de capacités, les deux groupes ont noté la nécessité de prendre en compte les contextes nationaux et régionaux, et que les principes d'appropriation nationale, de transparence et de durabilité doivent être respectés. Il est également apparu clair à ces deux groupes que les activités de renforcement de capacités devraient être coordonnées, afin d'éviter la duplication des efforts. Cependant, ces deux groupes ne se sont pas positionnés sur comment appliquer le droit international au cyberespace. ***Lisez nos rapports depuis les consultations du GTO.***

Il est souvent dit que les travaux du GTO et du GEG doivent être complémentaires. Pourtant, des divergences demeurent par rapport à ce que devrait être leur rôle respectif. Au cours des consultations informelles du mois de décembre, il semblerait qu'il soit possible d'éviter de dupliquer leurs efforts, mais on ne sait pas encore ce qui s'est passé derrière les portes closes de la première réunion de fond du GEG du 9 au 13 décembre.

2. Lutter contre la désinformation en temps d'élections : interdire les contenus politiques et limiter le micro-ciblage des publicités politiques

Préoccupés que la désinformation puisse influencer les processus électoraux et affaiblir la confiance dans la démocratie, les gouvernements ont augmenté la pression sur les entreprises de l'Internet. En réponse, les entreprises ont commencé à mettre à jour leurs politiques internes sur la publicité et la mise en ligne de contenus politiques.

Twitter a adopté une approche ferme en instituant une interdiction de la promotion payante de contenus politiques. Cela inclut les contenus qui font référence à un candidat, un parti politique, un représentant gouvernemental élu ou désigné, des élections, référendums, des sondages, ou le résultat de processus législatifs. Le dirigeant de Twitter Jack Dorsey a expliqué que si les « followers » acceptent implicitement les messages politiques quand ils décident de choisir un compte, cette prise de décision ne doit pas être compromise par de l'argent (c'est-à-dire des publicités payantes).

Les réactions à l'interdiction de Twitter sont mitigées. Certains ont salué cette décision ; d'autres l'ont jugé trop

sévère et simpliste, car elle désavantage les nouveaux venus au monde politique et fait de Twitter l'arbitre de ce qui est ou n'est pas un discours politique.

Google a opté pour un changement de politique moins drastique : les publicités électorales doivent désormais seulement utilisées des données générales (âge, genre, et localisation générale) pour cibler leur public. L'entreprise a également expliqué qu'elle n'a jamais autorisé le micro-ciblage granulaire – une pratique permettant aux publicitaires d'envoyer des messages à des groupes d'individus très limités – de publicités politiques sur ses plateformes.

Avant les annonces de Google et Twitter, la position de Facebook a été de ne pas interférer avec la publicité politique, afin de protéger la liberté d'expression et éviter les ambiguïtés sur ce qui définit l'expression politique. Mais l'entreprise fait face à une pression croissante en faveur de nouvelles mesures et envisage désormais de prévenir le micro-ciblage des annonceurs politiques (par exemple en augmentant le nombre minimal d'individus qu'un message politique peut viser, en passant de 100 à plusieurs milliers).

Les différentes positions adoptées par les principales entreprises de l'Internet laissent des questions ouvertes : L'interdiction de Twitter sera-t-elle plus efficace que l'approche de Google et Facebook sur le ciblage des utilisateurs par des publicités politiques ? Les entreprises doivent-elles déterminer ce qu'est un contenu politique ? Est-ce suffisant de mandater les entreprises à lutter contre la désinformation, ou est-ce qu'une réglementation plus stricte doit être imposée ? Si une réglementation est à souhaiter, quelle serait-elle ?

3. Lutter contre les deepfakes : outils technologiques et initiatives politiques

Les deepfakes utilisent les technologies de réseaux neuronaux et de machine learning pour falsifier les images et vidéos afin de faire faussement croire que quelqu'un a dit ou fait quelque-chose.

Les deepfakes peuvent être abusés dans différents contextes : pour discréditer des opposants au cours de campagnes politiques, pour attaquer la réputation personnelle (par exemple en faisant apparaître des individus dans des vidéos pornographiques où ils ne se trouvent initialement pas), et également pour aggraver des crises menant parfois à des conflits violents. Alors que cette technologie devient de plus en plus sophistiquée et accessible, les entreprises du numérique et les gouvernements cherchent à trouver des solutions à ces nouveaux défis.

La technologie elle-même offre plusieurs solutions. Les mêmes outils d'intelligence artificielle (IA) qui permettent de générer ces deepfakes peuvent être utilisés pour les détecter. Google et Facebook ont développé des répertoires de fausses vidéos et les ont mis à disposition des chercheurs développant des outils de détection. Facebook a même lancé un Deepfake Detection Challenge. La technologie de la blockchain a également été suggérée comme possible solution dans la lutte contre les deepfakes : l'authenticité des images et des vidéos peut être établie à travers une application blockchain qui compare le code hash cryptographique de certains fichiers avec celui des originaux.

Les solutions technologiques ne seront cependant pas forcément suffisantes pour contrer les risques liés aux deepfakes, notamment car les méthodes de détection ont tendance à être en retard sur les techniques de création. Mais les politiques des entreprises et les textes législatifs pourraient complémenter ces solutions techniques. Twitter a par exemple annoncé travailler sur une politique de lutte contre les deepfakes et les médias de synthèse sur sa plateforme. La Chine a adopté de nouvelles réglementations pour interdire la distribution de deepfakes sans que ne soit révélé le contenu qui a été détourné. Le non-respect de cette obligation sera puni d'une condamnation pénale à partir de janvier 2020. Certaines législations déjà en place pourraient également être utiles : la Californie a par exemple déjà criminalisé la publication de faux enregistrements audio, d'images ou de vidéos durant des campagnes politiques.

Mais ce qui est certain, c'est qu'au-delà des outils techniques et nouvelles réglementations, la lutte contre les abus liés aux deepfakes va nécessiter un travail de sensibilisation des utilisateurs. Un public informé, maîtrisant les outils numériques et suffisamment critique, sera évidemment central pour assurer que l'Internet développe tout son potentiel, en tant que vecteur positif de changement.

Les deepfakes peuvent être abusés pour discréditer des adversaires politiques
Credit: ColdFusion YouTube – capture d'écran

Les développements de politiques numériques en novembre et décembre

Avec tant de développements chaque semaine, l'environnement politique est rempli de nouvelles initiatives, d'évolutions réglementaires, de nouvelles décisions de justice, et de changements géopolitiques.

A travers l'observatoire *Digital Watch*, nous décodons, contextualisons, et analysons ces développements, dans un format simple. Le baromètre du mois suit et compare ces développements afin de distinguer des tendances et la présence de nouveaux sujets à l'agenda par rapport au mois précédent. Ce baromètre les résume, mais n'hésitez pas à cliquer sur les icônes en bleu pour en apprendre plus, ou visiter la section Updates de l'observatoire.

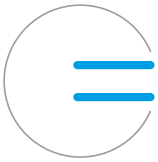
En progression

Architecture globale de la gouvernance de l'Internet

Le 14ème Forum sur la gouvernance de l'Internet (FGI) a rassemblé plus de 3000 participants pour échanger sur les défis actuels relatifs à la gouvernance des données, l'inclusion numérique, la sécurité, la stabilité et la résilience. *En savoir plus en pages 6-7.*

La World Wide Web Foundation a lancé le *Contrat pour le Web*, qui formule neuf principes pour protéger le Web en tant que vecteur positif.

La Coalition Just Net a publié le *Manifeste Digital Justice* qui traite des discussions sur la gouvernance des données dans le contexte de la justice sociale, l'équité et les biens communs.



Neutre

Développement durable

Le rapport de l'Union Internationale des Télécommunications (UIT) *Mesurer le développement numérique: faits et chiffres 2019* confirme les obstacles actuels à l'accès à Internet et à son utilisation, notamment dans les pays les moins développés.

Le rapport 2019 sur le développement humain a appelé à des politiques et incitations pour exploiter la puissance des technologies numériques afin de réaliser les objectifs sur le développement durable (ODD).

En progression

Sécurité

Le troisième comité de l'AGNU a adopté une résolution pour lutter contre l'utilisation des TIC à des fins criminelles. Les BRICS (Brésil, Russie, Inde, Chine et Afrique du Sud) ont souligné le rôle central que l'ONU doit jouer pour développer les normes sur le comportement responsable des Etats dans le cyberespace. Les groupes de l'ONU GEG et GTO ont tenu des consultations avec des parties non-membres sur des questions relatives au comportement responsable des Etats dans le cyberespace. Une session du GEG s'est également réunie.

La Commission mondiale sur la stabilité du cyberespace a proposé un cadre sur la cyber stabilité et huit normes volontaires pour mieux garantir la stabilité du cyberespace. Facebook a décidé de mettre en place le chiffrement de bout-en-bout sur ces applications de messagerie. Plusieurs cyber-attaques ont été révélées à travers le monde, visant des systèmes gouvernementaux dans le territoire canadien de Nunavut, l'Etat américain de la Louisiane, et la ville de New Orleans ; un hôpital en France, des installations nucléaires en Inde et au Royaume-Uni, et le parti du Labour britannique.

En progression

E-commerce et commerce en ligne

L'administration des transports de Londres a décidé de ne pas délivrer à Uber une nouvelle licence pour opérer dans cette ville.

Le gouvernement tchèque a proposé une taxe de 7% sur les géants de l'Internet. L'Inde a exprimé son insatisfaction par rapport à l'approche unifiée prise par le secrétariat de l'OCDE en matière de taxation de l'économie numérique. Au cours des élections canadiennes, le parti libéral a proposé une taxe sur les services numériques.

Les pays membres de l'Organisation mondiale du commerce (OMC) ont approuvé de conserver la pratique actuelle, qui vise à ne pas imposer de droits de douane sur les transmissions électroniques.

En progression

Droits numériques

Le rapport de Freedom House, qui s'intitule *Freedom of the Net 2019*, illustre la détérioration de l'état des libertés numériques à travers le monde.

La Commission européenne entend présenter une version révisée de sa proposition de règlement ePrivacy. Le parlement indien débat actuellement sur une nouvelle loi en matière de protection des données.

Twitter a annoncé une mise à jour de sa politique de vie privée et lancé un centre pour la vie privée.

Des perturbations de l'Internet et des blocages ont été enregistrés en Iran et en Irak.

Twitter a annoncé une interdiction de presque toutes les publicités politiques sur sa plateforme. Google limite les publicités à celles qui n'utilisent que des données générales pour cibler le public. Facebook considère la mise en place de limitations sur le micro-ciblage de publicités politiques.

Neutre

Questions légales

Une proposition de loi au Sénat américain vise à rendre illégal le stockage par des entreprises américaines de données d'utilisateurs ou de clés de chiffrement en Chine.

La Federal Trade Commission (FTC) devrait étendre son enquête en matière de concurrence aux activités cloud d'Amazon.

Huawei a porté plainte devant une Cour américaine contre la Federal Communications Commission (FCC) pour avoir injustement interdit les opérateurs ruraux de demander des subventions du gouvernement pour acheter des équipement de l'entreprise chinoise.

En progression

Infrastructure

Le RIPE Network Coordination Centre (RIPE NCC) a épuisé son pool d'adresses IPv4.

Internet Society a annoncé la vente du registre .org à la société financière privée Ethos Capital, suscitant des inquiétudes sur une hausse des prix et de potentielles implications pour les droits de l'homme.

Microsoft entend adopter le standard de sécurité DNS-over-HTTPS (DoH) par défaut sur Windows 10.

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a publié un rapport évaluant les menaces sur le réseau 5G.

En baisse

Neutralité du net

Une coalition d'entreprises technologiques et de défenseurs de l'intérêt public a demandé à la Cour d'appel américaine de réviser une décision qui maintient l'abrogation par la FCC des règles de neutralité du net.

Neutre

Nouvelles technologies (internet des objets, IA, etc.)

L'Australie a publié une série de principes éthiques pour l'IA. Le président russe Vladimir Poutine a appelé à des règles morales pour les interactions hommes-machines.

La Confédération des laboratoires sur l'IA en Europe (CLAIRE), lancée à la Haye, va travailler sur l'IA centrée sur l'homme.

Le Parlement allemand a adopté des règles autorisant les banques à être dépositaire de fonds de monnaies virtuelles. La Banque centrale française examine actuellement la possibilité de délivrer des monnaies virtuelles. Le Conseil européen et la Commission européenne ont souligné qu'aucun crypto actif à valeur stable ne verrait le jour au sein de l'UE tandis que les problématiques légales et réglementaires seront suffisamment prises en compte.

Berlin 2019: l'aube d'un nouveau FGI ?

Le Forum sur la gouvernance de l'Internet (IGF) s'est réuni pour la 14ème fois à Berlin du 25 au 29 novembre 2019. Ayant pour thème *« Un monde. Un réseau. Une vision »*, cet évènement a réuni un nombre record de plus de 3000 participants pour échanger non seulement sur les questions numériques d'actualité, mais aussi sur le futur du FGI.

La gouvernance des données, l'inclusion numériques et la sécurité

Le FGI 2019 a porté sur trois grands thèmes : la gouvernance des données, l'inclusion numériques, et la sécurité, la stabilité et la résilience. Cette thématisation claire a permis d'avoir des discussions plus productives, et plusieurs conclusions ont ainsi pu émerger.

Les débats sur la **gouvernance des données** ont porté sur deux nécessités concurrentes : la libre circulation des données à travers les frontières et la localisation des données. Certains ont souligné l'importance de la libre circulation des flux de données et son rôle essentiel pour permettre le développement social et économique. D'autres ont mis en exergue des préoccupations d'ordre politique, sécuritaire et économique pour justifier une priorisation des politiques de localisation des données. Mais des propositions dépassant cette opposition binaire ont aussi été entendues. Des solutions constructives de gouvernance des données peuvent être développées en distinguant les différents types de données (personnelles, scientifiques, publiques) et les différents garde-fous et politiques nécessaires. Cette approche offre la possibilité de cadres de gouvernance qui reflètent les différents besoins des individus, organisations de recherche, entreprises et gouvernements.

Les discussions sur **l'inclusion numérique** ont commencé par reconnaître qu'une approche holistique était nécessaire : l'inclusion nécessite de garantir l'accès à des réseaux et terminaux, mais ne s'y limite pas. Des réseaux de communautés, les partenariats public-privés, et les incitations financières font partie des mesures pouvant contribuer à créer des infrastructures réellement résilientes.

Une fois mises en place, des politiques et initiatives sont nécessaires pour permettre un accès abordable, l'éducation, l'inclusion financière, l'égalité de genre, et la disponibilité des contenus en ligne dans les langues locales. De plus, une réelle inclusion numérique ne sera réalisée que si les utilisateurs des technologies sont en mesure de les utiliser afin de répondre au mieux à leurs besoins (en matière d'informations, d'éducation, d'opportunités économiques...)

Le rôle des cyber-normes pour assurer la sécurité et la stabilité du cyberespace a dominé les discussions en matière de **cyber sécurité**. Les normes volontaires peuvent aider à soutenir un comportement responsable des Etats et des autres acteurs du cyberespace. Mais des préoccupations demeurent par rapport à la duplication des efforts à travers les différents forums, à la participation limitée de certains acteurs, et au manque de mécanismes institutionnels pour suivre la mise en œuvre et conformité. Et si il existe un certain consensus sur le fait qu'en théorie, le droit international s'applique au comportement responsable des Etats dans le cyberespace, plus de travaux sont nécessaires pour comprendre ce que cela veut dire en pratiques.

Rendre le cyberespace plus sûr est une responsabilité commune. Le comportement responsable des Etats est une nécessité claire, tout comme le sont des réglementations adéquates, la mise en œuvre de standards de sécurité dans l'infrastructure numérique, la sensibilisation aux questions de cybersécurité et le renforcement de capacités des utilisateurs, et la coopération multipartite. Les approches de cyber stabilité doivent trouver un équilibre entre les mesures pour la cyber sécurité et la nécessité de protéger les droits de l'homme, l'éthique et la confiance.

D'une IA fiable au renforcement des PME

Si ces trois thèmes étaient au centre des sessions de ce FGI 2019, de nombreux autres ont également été mentionnés. Les rapports de session et analyses de données de GIP révèlent les différentes questions traitées et conclusions auxquelles ont abouti ces discussions. Vous trouverez ci-dessous un sommaire de ces discussions, mais pour une liste plus exhaustive, rendez-vous sur notre Rapport Final du FGI 2019.

- Nous devons permettre le développement et déploiement de systèmes d'IA fiables pour le bénéfice de tous. Appliquer les principes d'inclusivité, de transparence, et assurer le respect des cadres établis de protection des droits de l'homme sont nécessaire pour permettre que l'IA n'aggrave pas les inégalités sociales et la fracture numérique.
- Une action plus décisive est nécessaire pour s'assurer que les enfants soient en sécurité en ligne et leur permettre d'exercer leurs droits en ligne. Des mesures possibles incluent des programmes pédagogiques, des outils techniques pour le contrôle parental, et le renforcement de réglementations pour protéger les mineurs. De même, les besoins des femmes, minorités, et personnes en situation de handicap doivent être mieux pris en compte par les entreprises et régulateurs.

ORGANISATION INTERNATIONALE DE la francophonie

La version française de la newsletter Digital Watch a été publiée avec le soutien de l'Organisation internationale de la Francophonie www.francophonie.org

ACTUALITE NUMERIQUE DE LA FRANCOPHONIE

Les enjeux numériques sont au cœur des priorités de la Secrétaire générale de la Francophonie, Mme Louise Mushikiwabo. Cette priorité se traduit à la fois dans l'action intergouvernementale et dans les actions au plus près des populations et des opérateurs économiques.

Ainsi, la récente conférence ministérielle de la Francophonie tenue à Monaco à la fin du mois d'octobre 2019 a entériné la création d'un groupe de travail sur le numérique qui se réunira à échéance régulière à Paris, au siège de l'Organisation internationale de la Francophonie, et dont les travaux seront complémentaires de ceux de la Commission économique de la Francophonie. Cette initiative a été saluée par les pays membres, très favorables à un engagement soutenu de l'OIF autour des enjeux numériques.

Dans ce contexte, le thème du prochain Sommet des chefs d'Etat et de gouvernement de la Francophonie, qui se tiendra à Tunis les 12 et 13 décembre prochains, a été officiellement dévoilé lors de cette Conférence de Monaco. Comme l'annonce le titre, « **Connectivité dans la diversité : le numérique vecteur de développement et de solidarité dans l'espace francophone** », le numérique sera au cœur des discussions au plus haut niveau des instances de la Francophonie. Ainsi, l'OIF, et les autres opérateurs de la Francophonie, se projettent résolument vers l'avenir l'année où l'organisation fête ses 50 ans.

Au-delà des projets de terrain menés par l'OIF dans le domaine du numérique, tournant notamment autour des accélérateurs et incubateurs, ou de l'entreprenariat et notamment l'entreprenariat féminin, la Représentation permanente de la Francophonie à Genève a conduit du 13 au 15 novembre 2019 une initiative pilote, saluée par les institutions partenaires : le premier atelier de formation conjointe des négociateurs commerciaux, climatiques et numériques de l'espace francophone. Six pays de la Francophonie (Maroc, Côte d'Ivoire, Mali, Bénin, République centrafricaine et République Démocratique du Congo) ont désigné un(e) négociateur/négociatrice par secteur pour prendre part à cet exercice inédit, développé en partenariat avec la Conférence des Nations unies sur le commerce et le développement (CNUCED), le Programme des Nations unies pour l'environnement (PNUE), la Convention-cadre des Nations unies sur les changements climatiques (CCNUCC), le Centre de politique de

sécurité, Genève (GCSP), l'Institut de hautes études internationales et du développement (IHEID) et l'Institut des Nations unies pour la formation et la recherche (UNITAR). Les délégués des Missions permanentes à Genève des pays de la Francophonie se sont aussi joints à l'exercice.

Au-delà, d'une sensibilisation de chaque expert aux domaines de négociation qu'il maîtrise moins, l'atelier a voulu mettre l'accent sur les convergences entre les sujets, ainsi que les actions conjointes qui peuvent être menées au niveau national comme international. L'atelier s'est conclu par un exercice de simulation de négociation mêlant ces différentes dimensions.

Dans cet effort de briser les silos et d'intégrer les différentes stratégies nationales de négociation sectorielle, la dimension numérique est apparue comme indispensable, à la fois comme accélérateur des mutations et moteur de développement. Le numérique est désormais totalement transversal et cette transversalité doit se traduire en actions concrètes de gouvernance internationale, et notamment dans une meilleure convergence des politiques commerciales et des politiques environnementales.

Le numérique, sous l'angle du commerce électronique, a également fait l'objet de nombreuses discussions lors de la concertation des pays francophones d'Afrique pour la préparation de la XIIe Conférence ministérielle de l'OMC qui s'est tenue du 9 au 11 décembre dernier à Marrakech (Maroc). Plusieurs pays francophones ont souligné leur intérêt pour les discussions plurilatérales qui se sont engagées depuis avril 2019 à l'OMC sur le commerce électronique. Mais ils ont également souligné combien ils estimaient ne pas encore avoir une bonne compréhension des enjeux et de l'état de leur secteur. L'objectif de la Francophonie est d'apporter en 2020 une assistance à ces pays afin qu'ils puissent souverainement prendre leurs décisions dans ce domaine sur la base d'informations fiables.

- Si la plupart s'accorde pour dire que le cyberespace bénéficierait de plus de régulation dans des domaines tels que les droits numériques, la cybersécurité et des contenus illégaux en ligne, la forme d'une telle régulation reste sujette à débat. Ces régulations devraient trouver un point d'équilibre entre les droits et intérêts des différents acteurs (par exemple, protéger les droits des utilisateurs, tout en encourageant l'innovation), le respect des principes démocratiques, et reposer sur des processus inclusifs et multipartites.
- Maximiser l'interopérabilité et l'harmonisation entre les cadres réglementaires et légaux nationaux est nécessaire pour empêcher la fragmentation du cyberespace. Cela permettrait également d'accroître la sécurité légale pour les entreprises et faciliter les opérations transfrontalières.
- Une économie numérique en croissance doit pouvoir donner des opportunités aux petites et moyennes entreprises à travers les outils numériques. Cet environnement doit par exemple permettre un accès aux infrastructures numériques (à travers plus de connectivité, de cloud computing, et services de paiement en ligne), un accès au financement, et des politiques fiscales encourageant l'investissement.
- Pour lutter contre la désinformation et les contenus violents en ligne, les mesures auto-réglementaires (par exemple, des politiques de contenu strictes, des codes de conduite, des mesures techniques telles que des algorithmes pour identifier et supprimer le contenu nuisible) sont probablement insuffisantes. Les entreprises technologiques sont sous une pression accrue pour augmenter leurs efforts et développer de nouvelles solutions, et si ces dernières s'avèrent inadéquates, les gouvernements sont prêts à adopter des réglementations plus contraignantes.

Le futur du FGI: mettre en œuvre un FGI Plus?

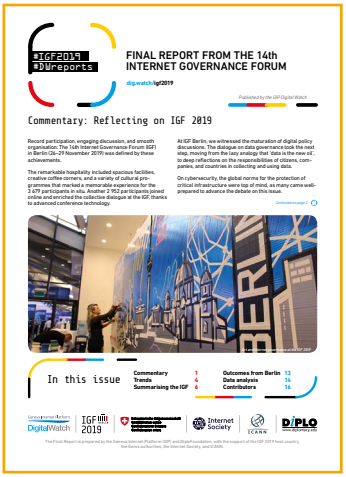
Cette édition du FGI a représenté un véritable pas en avant. Le programme plus concentré de cette année a permis des discussions politiques plus approfondies et plus poussées. Le nombre record de participants et la présence d'acteurs d'habitude moins représentés (comme les parlementaires, et les acteurs du Sud) ont donné une nouvelle énergie et profondeur aux débats. La présence du secrétaire-général de l'ONU António Guterres et de la chancelière allemande Angela Merkel a démontré le soutien de haut-niveau à ce forum. L'excellente organisation et les installations remarquables ont permis de faire de cet événement un réel succès.

Mais est-ce que le succès du FGI 2019 sera suffisant pour garantir la pertinence du FGI dans l'écosystème en constante évolution de la gouvernance de l'Internet et des politiques numériques ? La réponse est probablement non, en particulier au regard de la faible visibilité du Forum en dehors des cercles habituels. Ainsi, il est peu probable que les résultats de cet évènement (à travers ses messages, sommaire de la présidence, et du forum sur les bonnes pratiques) soient abordés lors de réunions de conseils d'administration d'entreprises ou dans des cabinets ministériels à travers le monde.

Mettre en œuvre les éléments du modèle IGF Plus proposé dans le rapport du Groupe de haut niveau sur la coopération numérique du Secrétaire général de l' ONU pourrait être la solution. Ce modèle a suscité d'intenses discussions à Berlin et a reçu un large soutien, étant considéré comme la voie à suivre la plus appropriée, afin de rendre le FGI plus robuste et pertinent, mais aussi pour renforcer le cadre pour la coopération numérique au niveau international.

Plus de discussions sont encore nécessaires pour la mise en œuvre du modèle FGI Plus. Comment préserver la ferveur de la participation multipartite et l'ouverture des réunions annuelles tout en produisant des résultats plus tangibles ? Est-ce que le FGI peut délivrer des recommandations politiques sans devenir une organisation de prise de décision ? D'où viendront les fonds supplémentaires pour soutenir le modèle FGI Plus ? Si ces questions et d'autres trouvent réponse, avec suffisamment d'urgence et de responsabilité, alors des éléments de ce nouveau modèle seront peut être visibles lors du prochain FGI l'année prochaine à Katowice.

L'observatoire *GIP Digital Watch* a offert une couverture en direct au cours du FGI 2019. Visitez la page dédiée – **dig.watch/igf2019** – pour accéder aux rapports de presque l'intégralité des sessions, les briefs journaliers récapitulant les discussions, des analyses de données, des interviews vidéo, et le rapport final du FGI 2019. L'initiative de reporting instantané a été réalisée en collaboration avec le pays hôte du FGI 2019, Internet Society, les autorités suisses et ICANN.


#igf2019 #DWreports

FINAL REPORT FROM THE 14th INTERNET GOVERNANCE FORUM

dig.watch/igf2019

Published by the GIP Digital Watch

Commentary: Reflecting on IGF 2019

Record participation, engaging discussions, and smooth organisation: The 14th Internet Governance Forum (IGF) in Berlin (25–29 November 2019) was defined by these achievements.

The remarkable hospitality included spacious facilities, creative coffee corners, and a variety of cultural programmes that marked a memorable experience for the 3 079 participants in situ. Another 2 952 participants joined online and enriched the collective dialogue at the IGF, thanks to advanced conference technology.

At IGF Berlin, we witnessed the maturation of digital policy discussions. The dialogue on data governance took the next step, moving from the hazy analogy that 'data is the new oil', to deep reflections on the responsibilities of citizens, companies, and countries in collecting and using data.

On cybersecurity, the global norms for the protection of critical infrastructure were top of mind, as many came well-prepared to advance the debate on this issue.

Continued on page 2

In this issue

Commentary 1
Trends 4
Summarising the IGF 4
Outcomes from Berlin 13
Data analysis 14
Contributors 16

The Final Report is prepared by the Geneva Internet Platform (GIP) and DiploFoundation, with the support of the IGF 2019 host country, the Swiss authorities, the Internet Society, and ICANN.

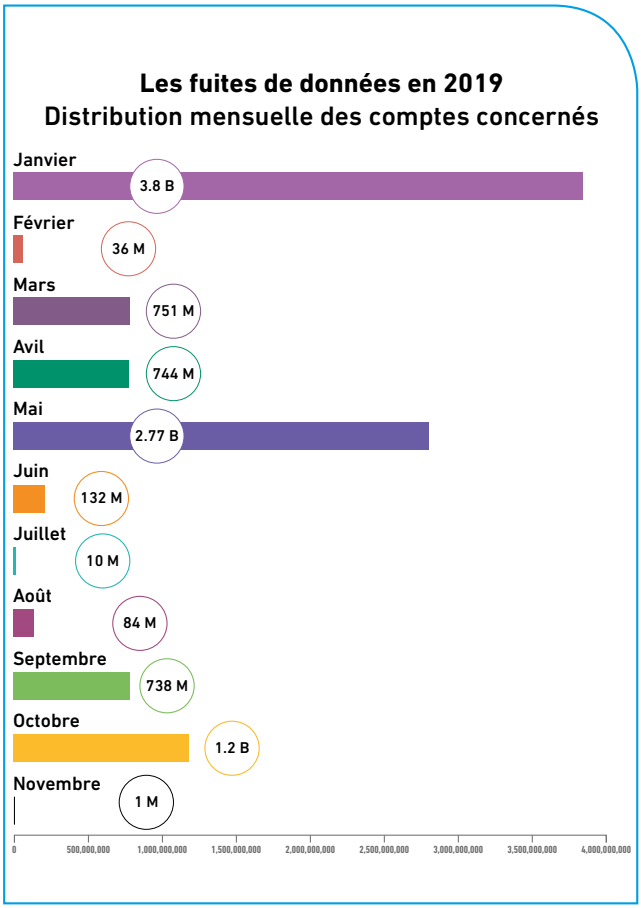
Tout ce que je veux pour Noël, c'est... des données

Avec seulement quelques jours avant 2020, il est le temps de revenir sur l'année écoulée. Quelle meilleure façon de le faire qu'en s'intéressant aux principaux chiffres de l'année.

Dans les numéros précédents de la newsletter, nous nous sommes intéressés à la protection et aux violations des droits de l'homme en ligne. Certains numéros ont porté sur les récentes enquêtes lancées en matière de protection des données personnelles, au regard du règlement général sur la protection des données (RGPD), et l'état des lieux des blocages de l'Internet. Cette fois nous nous intéressons à un autre sujet qui peut nous affecter d'une manière ou d'une autre, les fuites de données.

Les données comme ressources

Les données sont désormais considérées comme la ressource avec le plus de valeur. Les hommes ont toujours tendances à utiliser des métaphores du monde réel pour représenter de nouvelles idées et disciplines, et notre approche aux données n'est pas différente. Le pétrole, le bacon, l'or, font partie des analogies utilisées pour évoquer la valeur des données pour la société et l'économie. Une autre image est celle du tsunami de données qui décrit à la fois le flux d'informations auxquelles nous sommes maintenant exposées et l'accessibilité croissante de nos données personnelles en ligne. Une autre image est celle des déchets nucléaires, qui bien que sombre, possède sa part de vérité. Comme les déchets nucléaires, une fois que les données fuitent, les problèmes sont dangereux, durables, et c'est un point de non-retour.



Protéger les données contre les fuites

Dans nos sociétés de plus en plus numériques, les données personnelles sont collectées, stockées, et traitées dans un grand nombre de domaines. Les agences gouvernementales stockent et traitent des données en matière de santé, de sécurité sociale, de fiscalité, et d'éducation. Les entreprises et organisations traitent des données personnelles de leurs employés et contractants. Et les entreprises de l'Internet collectent et utilisent des données personnelles selon des objectifs dont ne nous sommes parfois pas conscients.

De nombreuses juridictions à travers le monde ont un cadre réglementaire et légal pour le traitement de données personnelles, obligeant les organisations à respecter un certain niveau de confidentialité et d'intégrité de leurs systèmes. Le RGPD est de plus en plus perçu comme le standard à suivre en matière de vie privée et de protection des données, et à inspirer plusieurs cadres de protection à travers le monde. C'est par exemple le cas de la nouvelle réglementation en matière de protection des données en Californie, le Californian Customer Privacy Act, et d'un nouveau texte de loi en Inde en la matière.

Mais pour quel impact ? Quelle est la sécurité de nos données par rapport à des fuites ou des révélations non-autorisées ?

Les fuites de données en 2019

Bien qu'il soit difficile de donner le nombre exact de fuites de données, car nombre d'entre elles ne sont pas toujours reportées, notre analyse du paysage de la cybersécurité a observé plus de cent incidents d'ampleur en 2019 (notre analyse se fonde sur des informations de plusieurs sources numériques comme Have I Been Pwned et Selfkey).

Notre conclusion est qu'environ 10 milliards d'informations ont été publiquement exposées, ce qui représente une augmentation de plus de 100% par rapport à l'année

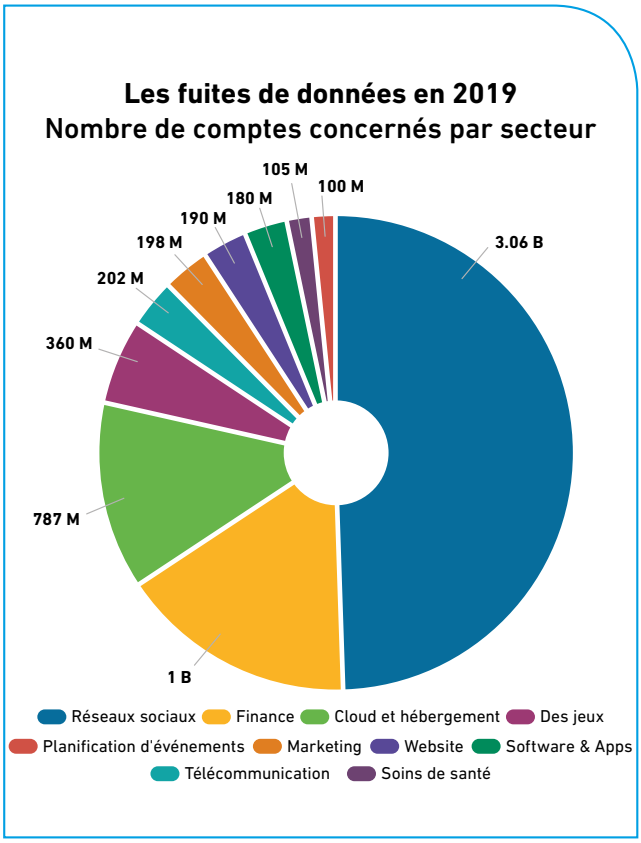
2018. L'entreprise Risk Based Security corrobore nos résultats en indiquant que 2019 est une année record en termes de fuites de données.

Les principales fuites ont été permises par des sources anonymes, qui ont révélé au total environ 3 980 000 000 dossiers. L'industrie le plus affectée par ces fuites a été l'industrie de la santé, ce qui est très préoccupant. Ce n'est cependant pas le seul secteur qui laisse les données personnelles vulnérables. La majorité des divulgations – environ 3 milliards – provenait de fuites de données sur les réseaux sociaux.

Le tableau ci-dessous détaille les 26 industries affectées par des fuites de données dans le monde. La grande majorité des incidents a eu lieu dans la première moitié de l'année, avec 69 incidents, en comparaison aux 32 dans la seconde.

Les fuites de données ont des causes multiples. Des fois, les organisations traitant les données n'ont pas des mesures techniques adéquates, rendant leurs systèmes vulnérables à des cyberattaques. Les bases de données, les sauvegardes et les services mal configurés ou mal sécurisés sont parmi les causes d'incidents les plus fréquents.

Il y a aussi un facteur humain possible, qui est habituellement considéré comme le principal motif des failles de cybersécurité. Les pertes de données, et autres types d'erreurs humaines, sont les plus fréquentes. Selon des données compilées par l'entreprise Kroll, 90% des fuites de données signalées à l'autorité de protection britannique entre 2017 et 2018 ont été causées par une erreur humaine.



Top des fuites de données en 2019

- La banque américaine Capital One a vu les données de plus 100 millions de citoyens américains et 6 millions de résidents canadiens volées par un hacker, avec notamment 140000 numéros de sécurité sociale, et 80000 numéros de comptes bancaires.
- En Inde, une base de données non protégée du Département de la santé et de la famille a mis en ligne les données médicales de plus de 12.5 millions de femmes enceintes.
- Aux Etats-Unis, une fuite de données a affecté l'opérateur T-Mobile, exposant les données de plus de 1 million d'utilisateurs, et notamment leur nom, numéro de téléphone, et adresse.
- Un autre incident sérieux a touché l'entreprise d'analyse de données Ascension révélant les données financières de 24 millions d'individus (noms, adresses, numéros de sécurité sociale, comptes en banque d'institutions comme HSBC Life Insurance, CitiFinancial et Wells Fargo) sur une base de données non protégée pendant 2 semaines.
- Le Trésor bulgare a été victime de la plus grande fuite de données du pays, qui a compromis les données personnelles de plus de 5 millions de citoyens (numéros personnellement identifiables, adresse, revenu).
- Une attaque contre l'outil de design graphique Canva a affecté les comptes de plus de 139 millions d'utilisateurs, exposant leurs noms d'utilisateurs, adresses email et mots de passe.
- Le groupe hôtelier Marriott a fait part d'une attaque ayant touché les informations de plus de 383 millions de clients (notamment les informations de passeports, et de carte de crédit).
- Une fuite de données touchant Toyota a exposé les données personnelles de 3.1 millions de clients, notamment le nom, date de naissance et information professionnelle.

Existe-t-il une solution unique à tous ces problèmes ? Certainement pas. Alors que nous observons de plus en plus d'incidents, année après année, la véritable question n'est pas de savoir si une organisation sera affectée, mais plutôt quand. C'est pourquoi les organisations ne doivent pas seulement concentrer leurs efforts pour prévenir les fuites, mais aussi à en limiter l'impact.

Quant aux utilisateurs, il est maintenant grand temps de reconsidérer nos pratiques en matière de protection des données. Pour terminer l'année, nous devrions peut-être ajouter un nouvel élément à notre liste de bonnes résolutions – plus de vie privée en 2020.

Discussions de politiques numériques à Genève

De nombreuses discussions politiques ont lieu à Genève chaque mois. Les développements ci-dessous couvrent les principaux évènements du mois d'octobre. Pour lire les rapports de ces évènements, visitez la section *Past Events sur le site de l'observatoire Digital Watch.*

Semaine de la paix à Genève | 4–8 Novembre 2019

Cette conférence d'une semaine a souligné à la fois la capacité des technologies à améliorer la qualité de la paix, mais aussi affaiblir la paix et la sécurité. D'une part, les innovations des TIC ont offert de nouvelles opportunités pour les médiations de paix. D'autre part, le domaine du cyber est devenu un nouveau champ de bataille, conduisant de nombreux pays à développer de nouvelles capacités militaires, défensives et offensives. Ce nouveau paradigme du conflit international et de la guerre pose des questions urgentes en matière d'application des mécanismes légaux existants, comme le droit humanitaire international.

Lisez notre rapport de cette conférence.

Conférence CyberMédiation | 19 Novembre 2019

Cette conférence a porté sur l'utilisation des technologies numériques pour la médiation de paix et les opportunités et défis que représentent ces technologies. Traditionnellement, la médiation pour la paix s'est tenue dans des contextes confidentiels, en impliquant un nombre limité d'acteurs. Cependant, avec la prolifération des TIC et technologies numériques, on observe une évolution vers des approches plus inclusives et ouvertes. Cette conférence a mis en lumière la nécessité de planifier comment, et dans quelle mesure, les technologies numériques doivent être intégrées dans les processus de médiation. Pour répondre à ces questions, il sera nécessaire d'inclure toutes les parties prenantes.

FForum de l'ONU sur les entreprises et les droits de l'homme | 25–28 Novembre 2019

Sous le thème *« Il est temps d'agir : les gouvernements catalyseurs du respect des droits de l'homme par les entreprises »*, cette conférence a présenté les perspectives de tous les acteurs sur les efforts actuels et futurs pour la protection des droits de l'homme dans le contexte des activités commerciales. La cohérence politique des Etats membres de l'ONU et des outils d'évaluation ont été présentés comme nécessaire pour réaliser ces objectifs. L'esclavage numérique a fait l'objet d'une discussion en profondeur. Présentée comme une conséquence négative de la numérisation, les acteurs se sont accordés sur le fait que cette question devait être traitée au niveau local, national et global.

Sommet sur l'avenir du travail | 27 Novembre 2019

Organisé à l'occasion du centenaire de l'Organisation internationale du travail (OIT), ce sommet a abordé la nécessité de repenser les processus de collaboration et optimiser les outils numériques pour un futur du travail plus inclusif, productif et durable. Les discussions ont examiné comment la technologie transforme la façon de travailler des individus et les compétences nécessaires pour répondre à ces défis. Les débats ont également porté sur le potentiel de la technologie pour aider à réduire les inégalités, notamment le différentiel des taux d'emploi et de revenus entre les hommes et les femmes.

Forum sur le commerce mondial et la blockchain | 2–3 Novembre 2019

Organisée par l'OMC, cette conférence a présenté une série de cas d'utilisation de la technologie blockchain dans le commerce international. Cet évènement a abordé comment cette technologie pouvait être utile aux industries en matière de propriété intellectuelle, et le rôle que pouvait jouer la communauté internationale pour éviter de créer des barrières réglementaires non-nécessaires pour la blockchain et les technologies numériques. Cette occasion a aussi permis de discuter sur le rôle des organisations internationales pour promouvoir et développer un cadre réglementaire et politique pour permettre d'exploiter le potentiel des technologies, tout en maîtrisant leurs risques.

Les principaux évènements de politiques numériques en janvier

Nous analysons l'agenda des évènements de politiques numériques à venir afin d'identifier les discussions à suivre dans le courant des prochaines semaines.

Janvier

14–16 JANVIER
IGF 2020: Premières consultations ouvertes et réunion MAG (Genève, Suisse)

Le FGI va commencer les préparations pour sa prochaine réunion, qui se tiendra à Katowice, en Pologne du 2-6 novembre 2020. Une consultation ouverte avec la communauté du FGI sera suivie par une réunion du Multistakeholder Advisory Group (MAG). Les discussions porteront sur la structure et le programme du prochain FGI 2020, les activités intersessions, le rôle des FGI nationaux et régionaux, ainsi que les développements futurs possible pour le *modus operandi* du FGI.

20 JANVIER
Geneva Blockchain Congress (Genève, Suisse)

Le deuxième Geneva Blockchain Congress, dont le thème sera *« Du laboratoire au marché en passant par l'éthique, réglementation et gouvernance »*, portera sur une série de questions telles que : banque et finance, evolutions deep tech, santé et bien-être, commerce illégal et contrefaçon, administration publique, cadre réglementaire et légal, applications humanitaires et sociales, et logistique. D'autres discussions porteront sur la monnaie virtuelle de Facebook la Libra, la vie privée, la finance inclusive, et les identités numériques.

21–24 JANVIER
Réunion annuel du Forum économique mondial (Davos-Klosters, Suisse)

La 50ème réunion annuelle du Forum économique mondial aura pour thème *« Parties prenantes pour une cohésion et monde durable »*, et accueillera une série de discussions sur les technologies numériques, dans le contexte de la quatrième et cinquième révolution industrielle. La maison de la Suisse à Davos accueillera le lancement formel de la Swiss Digital Initiative Foundation[link] et une discussion sur « Comment gouverner l'interdépendance numérique ? », ainsi qu'une session intitulé « Road To Bern » en préparation du Sommet mondial des données de l'ONU à Berne en octobre 2020.

22–24 JANVIER
CPDP2020 Protection des données et intelligence artificielle (Bruxelles, Belgique)

L'édition 2020 de la conférence Ordinateurs, confidentialité et protection des données (CPDP2020) will aura pour thème *« Protection des données et intelligence artificielle »*. Organisé et soutenu par un consortium d'organisations – notamment Microsoft, Google, Facebook, la Commission européenne, l'Institut des Ingénieurs en Électronique et Électrique (IIEE), et des centres académiques d'excellence – CPDP2020 abordera la question de la réglementation de l'IA, l'impact de l'IA sur les droits de l'homme et la protection des données, les technologies de reconnaissance faciale et le RGPD.

28–30 JANVIER
Forum International de la Cybersécurité (Lille, France)

Ayant pour titre *« Placer l'être humain au cœur de la cybersécurité »*, l'édition 2020 du Forum International de la Cybersécurité (FIC) portera sur la sécurité et stabilité internationale, la lutte contre la cybercriminalité, la sécurité opérationnelle, le management des risques numériques, la confiance numérique, et la protection des données. Co-organisée par la Gendarmerie Nationale et European Strategic Intelligence Company (CEIS) avec le soutien de la Région Hauts-de-France, cette édition se tiendra pour la première fois pendant trois jours. Le premier jour sera dédié au commerce juste, et à un forum sur l'identité numérique. Les deuxièmes et troisièmes jours correspondront au forum principal.

Février

It's the end of the year as we know it (and we'll be fine)

Alors que nous faisions le bilan de l'année 2019, nous nous sommes dit que la meilleure façon de comprendre le monde complexe et en constante évolution de la gouvernance de l'Internet n'est peut-être pas à travers des graphiques et des statistiques, mais à travers un nuage de mots mis en musique. C'est donc avec grand plaisir que nous vous offrons la version révisée par *Digital Watch* du titre de REM, *It's the end of the world as we know it*, un véritable hit qui a marqué une génération, lorsque l'Internet était en plein développement. Nous vous recommandons de le chanter à tue-tête, et pourquoi pas d'ajouter vos propres paroles.

That's great, it starts with a debate
Talk of change, it's digital.
Connect me now, I'm lost in space
Include the lost, mind the cost.

Stop the hate, free the press
How can we clean up this mess?
Digital cooperation, awareness, education
Inclusion delusion disability reality.

Compact, convention, fake news, dissension
Relate co-operate exclusion confusion
Shut up shutdown who on earth is this clown?
Connection information cybercrime fragmentation.

ISOC ITU IPv6 who are you?
Copyright who's left? Gender rights left behind.
Rule of law democracy find sustainability.
Trust trust it's a must watch it now it's going bust
Network design Google has it – no, it's mine!
Cyberwar confrontation community opportunity.

It's the end of the year as we know it,
Gotta keep on working, don't you blow it.
It's the end of the year as we know it,
And I feel blind.
(gotta find some time offline)

Norms responsibility confidence security
Emerging submerging content dialects
Convergence divergence encryption and children
Ethics, trust, AI, do it now it will fly.

Greta Thunberg, DotOrg, HumAInism, 'holderism
Development #MeToo Who's in charge? Wish we knew
Stability legality taxes economy
Literacy inequality infrastructure, now you see.

Privacy, dignity, data, data, can't you see?
Algorithm, sing a song, bias has gotten it all wrong.
Technology, possibility, human computer, IoT.
We can do it, find the art. Common good, play the part.
IGF Plus Plus good idea, what's the fuss?
Listen to us outside, IQ'whalo cannot hide.

It's the end of the year as we know it,
Gotta keep on working, don't you blow it.
It's the end of the year as we know it,
We're gonna be fine
(See you next year online)

A propos de ce numéro
Le numéro 45 de la newsletter *Digital Watch*, publié le 20 Décembre 2019, par la Geneva Internet Platform et DiploFoundation | Contributeurs: Katarina Anđelkovic, Stephanie Borg Psaila (editor), Andrijana Gavrilović, Đorđe Jančić, Marco Lotti, Marilia Maciel, Nagisa Miyachi, Virginia Paque, Nataša Perućica, Sorina Teleanu | Traducteur de l'édition française: Clément Perarnaud | Design: Aleksandar Nedeljkov, Viktor Mijatović, et Mina Mudrić, Diplo's CreativeLab. | Contactez-nous: digitalwatch@diplomacy.edu

Allez en profondeur
Cliquez sur l'icône bleue lorsqu'elle apparaît dans la version numérique pour avoir accès à plus de ressources.

Sur la couverture
Berlin 2019: L'aube d'un nouveau FGI ? Credit: Vladimir Veljasević

Geneva Internet Platform DigitalWatch

La plateforme Internet de Genève est une initiative de:
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
REPUBLIQUE ET CANTON DE GENEVE
UNIVERSITÉ DE GENÈVE
ETH zürich
DiPLO www.diplomacy.edu