

## Facebook face aux critiques

### CONTENU

Les plateformes de réseaux sociaux ont des difficultés à supprimer les contenus préjudiciables. Sur la sellette : Facebook.

[Page 1](#)

### BOUCLIER DE PROTECTION DE LA VIE PRIVÉE III

Nous examinons les défis à relever pour parvenir à un accord sur les transferts de données personnelles.

[Pages 6-7](#)

### RANÇONGICIEL

31 pays et l'UE se sont réunis pour lutter contre les rançongiciels.

[Pages 8-9](#)

### METVERSE

La nouvelle "hype": De quoi s'agit-il et quels en sont les défis ?

[Page 10](#)

# Questions du moment en matière de politique numérique

## 1. Modération des contenus

La problématique de la modération des contenus a fait couler beaucoup d'encre en octobre. De nombreuses plateformes de réseaux sociaux ont dû faire face à des problèmes de modération des contenus et de réglementation. Microsoft retirera LinkedIn de Chine dans le courant de l'année [en raison de la pression exercée pour se conformer aux exigences du gouvernement chinois en matière de plateformes Internet](#). Les recherches internes de Twitter [ont permis de découvrir que ses algorithmes amplifient les contenus de droite - toutefois, l'entreprise ne sait pas pourquoi c'est le cas et va continuer à étudier la question](#). Mais aucune autre plateforme n'a eu un mois aussi difficile que Facebook.

Frances Haugen, ex-employée de Facebook devenue lanceuse d'alerte, a témoigné devant le Congrès américain que Facebook se préoccupe davantage des profits que des utilisateurs. [Elle a accusé Facebook de nuire à la santé mentale des enfants et d'amplifier la division, l'extrémisme et la polarisation parmi ses utilisateurs](#). Le témoignage de Haugen a été corroboré par un autre lanceur d'alerte [qui, au moment de la rédaction de cet article, est toujours anonyme](#). Devant le parlement britannique, Haugen a prévenu que le temps manquait pour réglementer les entreprises de médias sociaux qui utilisent l'IA pour la modération de contenu.

Un consortium d'agences de presse a obtenu des versions expurgées des documents divulgués par Haugen. Surnommés «The Facebook Papers», les documents montrent que l'entreprise rencontre de grandes difficultés pour lutter contre la désinformation liée aux vaccins [et à modérer les contenus dans des langues autres que l'anglais](#). [Ils indiquent également que Facebook a consacré nettement moins de ressources à la modération sur les marchés en dehors des États-Unis - seuls 13 % du budget consacré à la lutte contre la désinformation ont été dirigés au-delà des frontières américaines](#), où se trouvent 90 % de ses utilisateurs. En outre, les documents allèguent que Facebook a ignoré l'impact néfaste d'Instagram sur la santé mentale des adolescents [et a pris des mesures limitées pour mettre fin au trafic sexuel via la plateforme](#). Ses algorithmes alimentent la discorde, et ses stratégies sont insuffisantes pour endiguer les publications incitant à la violence dans les pays à risque de conflit.

Encouragés par les révélations concernant Facebook (bientôt Meta), les régulateurs du monde entier se préparent à une confrontation avec les plateformes de réseaux sociaux. TikTok, Snapchat et YouTube ont été interrogés par le Congrès américain sur la manière dont les enfants sont orientés vers des contenus spécifiques sur leurs plateformes. [Facebook, Google, Twitter et TikTok](#)

ont également témoigné sur la lutte contre les contenus préjudiciables devant le Parlement britannique. [L'Inde demande à Facebook des informations sur les algorithmes qu'il utilise pour modérer les contenus](#).

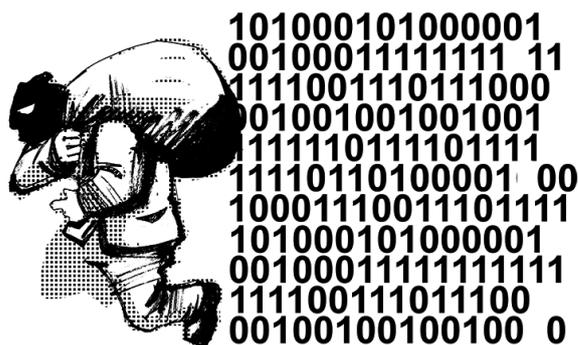
Légiférer est-il la solution ? Le Royaume-Uni et Singapour le pensent certainement : le premier va accélérer l'adoption de son projet de loi sur la sécurité en ligne, [et le second a adopté une loi](#) pour lutter contre les «interférences étrangères», qui permet aux autorités de bloquer les contenus qu'elles jugent hostiles.

Il est intéressant de noter que les géants de la technologie semblent sur la même ligne : Dans sa prise de position sur la protection de l'internet ouvert, Twitter a demandé que la réglementation définisse clairement les différentes catégories de contenu nécessitant une modération, en particulier lorsque le contenu est légal mais que «le gouvernement estime qu'il est nécessaire d'intervenir». Réagissant au témoignage de Mme Haugens devant le Congrès américain, Mark Zuckerberg, PDG de Facebook, a écrit que «l'organe approprié pour évaluer les compromis entre les équités sociales est notre Congrès démocratiquement élu». Il a exhorté le Congrès à mettre à jour les réglementations relatives à l'internet.

## 2. Contre les rançongiciels

Nous observons l'âge d'or des rançongiciels... ils sont devenus une priorité en matière de sécurité nationale... et certains affirment qu'ils n'ont pas encore atteint le sommet de leur impact, indique le rapport annuel de l'Agence européenne pour la cybersécurité (ENISA) sur les cybermenaces.

La raison pour laquelle les rançongiciels prospèrent est qu'ils ont été pour le moment largement incontestés, a déclaré Sir Jeremy Fleming, [responsable des questions cyber au Royaume-Uni](#). Il est légal de «s'en prendre» aux acteurs criminels en vertu du droit international, a déclaré M. Fleming, mais ce n'est pas si facile : «Il y a beaucoup de choses qui doivent être mises en place pour que cela se produise, et nous sommes loin de nous attaquer



réellement au modèle de profit qui rend leur exploitation si facile pour les criminels».

Les Pays-Bas et l'Australie sont favorables à des approches plus défensives. Ben Knapen, le ministre néerlandais des affaires étrangères, a fait remarquer que les voies diplomatiques et juridiques avaient la priorité, mais que les services de renseignement néerlandais pouvaient réagir à une attaque de rançongiciels menaçant la sécurité nationale. Le Defense Cyber Command peut même mener une contre-attaque, mais seulement en dernier recours, a souligné M. Knapen. L'Australie prévoit d'adopter une approche différente mais non moins intéressante. Selon le nouveau projet de loi sur les infrastructures critiques, l'Australian Signals Directorate (ASD) serait en mesure de prendre le contrôle des infrastructures critiques en cas d'attaque par rançongiciel. Une coalition d'entreprises a demandé des changements, réclamant un mécanisme d'examen et de contrôle judiciaire prévu par la loi et l'extension de la fenêtre de déclaration obligatoire d'un incident.

Les trois pays susmentionnés ont également participé à l'initiative *Counter Ransomware* menée par les États-Unis, qui a rassemblé 31 pays et l'UE et a abouti à des engagements en matière de lutte contre les rançongiciels au niveau transnational. *Pour en savoir plus sur cette initiative, voir les pages 8 et 9.*

Sur une note positive, le camp de la protection de la cybersécurité a remporté une grande victoire ce mois-ci : Le célèbre groupe de rançongiciels REvil, responsable du piratage de Kaseya et de JBS, a été piraté et mis hors ligne dans le cadre d'une opération menée dans plusieurs pays. Le groupe pourrait changer de nom, comme le font souvent les groupes de rançongiciels, mais les théories selon lesquelles il aurait perdu la confiance de la communauté cybercriminelle abondent.

### 3. Reconnaissance faciale : la vie privée dans le collimateur.

Tout au long de notre newsletter de juillet/août 2019, nous avons expliqué que les principales préoccupations autour de la technologie de reconnaissance faciale (TRF) étaient la vie privée, les préjugés et la discrimination. Ce mois-ci, les préoccupations relatives à la vie privée ont occupé le devant de la scène.

Les défenseurs de la vie privée craignent que le système de paiement par reconnaissance faciale du métro de Moscou ne soit utilisé par les agences de sécurité pour surveiller les citoyens. Il est vrai que le système semble puissant : il peut reconnaître les voyageurs même s'ils portent des masques ou des lunettes. Les autorités, quant à elles, se réjouissent que Moscou utilise désormais l'une des plus importantes utilisations du TRF au monde.

Les citoyens écossais n'ont pas été heureux d'apprendre que leurs données provenant de l'application Covid Status de NHS Scotland étaient partagées avec des entreprises technologiques, notamment la société de reconnaissance faciale par IA iProov. Le mécontentement s'est encore accru au Royaume-Uni lorsqu'on a appris que neuf écoles écossaises utilisaient des systèmes de TRF pour encaisser les paiements des repas des élèves. Les caméras du système vérifient les données biométriques des élèves stockés sur des serveurs dans les écoles. Le Bureau du commissaire à l'information du Royaume-Uni est intervenu, demandant instamment une alternative moins invasive pour le paiement.

Une unité de police finlandaise a été réprimandée par le médiateur adjoint pour la protection des données du pays pour le traitement illégal de données faciales. L'unité a expérimenté l'identification de possibles victimes d'abus sexuels sur des enfants en utilisant le logiciel Clearview AI. Clearview AI, dont le logiciel de reconnaissance faciale a fait l'objet d'une enquête pour avoir collecté des données sans discernement, a poursuivi son entreprise et collecté 10 milliards de photographies supplémentaires provenant des comptes publics sur des réseaux sociaux pour sa base de données.

Concernant le secteur privé, dans un cas sans précédent, le gouvernement sud-coréen a remis 170 millions de photographies collectées à l'aéroport international d'Incheon à des développeurs d'IA du secteur privé, sans le consentement des sujets.

Le vieux débat sur l'opportunité d'interdire ou de légiférer sur les TRF va continuer à faire rage, surtout si l'on considère les réactions de l'UE et des États-Unis au cours du mois dernier. Le Parlement européen a demandé l'interdiction de la reconnaissance automatisée dans les espaces publics de caractéristiques humaines telles que la démarche, le bout des doigts, l'ADN, la voix et d'autres signaux biométriques et comportementaux. Le Parlement a également demandé l'interdiction des bases de données privées de reconnaissance faciale (comme le système d'IA Clearview), des services de police prédictifs basés sur des données comportementales et de la notation massive des individus par l'IA.

De l'autre côté de l'Atlantique, le Bureau de la politique scientifique et technologique (OSTP) de la Maison Blanche américaine demande des informations sur les technologies, y compris les TRF, utilisées pour identifier les personnes et déduire leurs attributs. Selon l'OSTP, «au 21e siècle, nous avons besoin d'une «déclaration des droits» pour nous protéger des puissantes technologies que nous avons créées». Avant de rédiger un texte de loi essentiel, il est clair que les États-Unis cherchent à mieux comprendre cette technologie.

# Les développements de politique numérique qui ont fait la une

Le paysage des politiques numériques évolue quotidiennement. Voici donc les principaux développements du mois d'octobre. Nous les avons décodés en petites mises à jour faisant autorité. Vous trouverez plus de détails dans chaque mise à jour sur l'observatoire *Digital Watch*.



en baisse

## Gouvernance numérique mondiale

La Commission européenne a publié son plan de travail pour 2022, qui prévoit notamment de faire progresser le projet d'une « Europe adaptée à l'ère numérique ».

Les ministres du commerce du G7 se sont mis d'accord sur des principes pour régir le commerce numérique, couvrant des marchés numériques ouverts ; des flux de données transfrontaliers ; des garanties pour les travailleurs, les consommateurs et les entreprises ; des systèmes commerciaux numériques ; et une gouvernance mondiale équitable et inclusive.

Les dirigeants du G20 ont approuvé  l'accord de l'OCDE sur les règles fiscales mondiales.



en baisse

## Développement durable

L'ASEAN et les États-Unis ont publié une déclaration des dirigeants sur le développement numérique, s'engageant à coopérer en matière de cybersécurité, d'infrastructure numérique et d'économie numérique.

La Commission européenne a lancé un groupe d'experts chargé d'élaborer des lignes directrices sur la désinformation et la culture numérique à l'intention des éducateurs.



en progression

## Sécurité

Le gang de rançongiciel REvil a été piraté et mis hors ligne par un effort multinational. Le Royaume-Uni, l'Australie et les Pays-Bas ont détaillé leurs plans nationaux de lutte contre les rançongiciels. *Pour en savoir plus, voir les pages 2 et 3.*

L'initiative internationale *Counter Ransomware* a tenu sa première réunion. *Pour en savoir plus, voir les pages 8 et 9.*

Selon le rapport de l'ENISA sur les menaces de cybersécurité, les rançongiciels constituent la principale menace en Europe et les crypto-monnaies la principale méthode de paiement des acteurs de la cybermenace.

La Russie et les États-Unis ont coparrainé une résolution sur la cybersécurité à l'Assemblée générale des Nations unies, soulignant l'adoption de normes volontaires de comportement responsable.



en progression

## E-commerce et économie de l'internet

Un total de 136 pays a approuvé les nouvelles règles mondiales de l'OCDE en matière d'impôt sur les sociétés, qui affecteront les grandes entreprises technologiques.

La Chambre de commerce internationale a publié de nouvelles règles mondiales pour les transactions commerciales numériques.

Amazon a été accusé d'utiliser les données des vendeurs pour copier des produits et manipuler les résultats de recherche au profit de ces produits.

Le Nigeria a lancé eNaira, la première monnaie numérique du continent africain.



neutre

## Infrastructure

Facebook, WhatsApp et Instagram ont subi des pannes dans le monde entier en raison d'une configuration défectueuse des paramètres du protocole BGP (Border Gateway Protocol).

Le lancement de nouveaux câbles sous-marins est prévu, et comprennent le câble Afrique-Europe de Google, le câble Europe-États-Unis de Facebook et le câble 100 % vert Canada-Norvège d'Erikson.



neutre

## Droits numériques

La Commission européenne a lancé un groupe d'experts chargé d'élaborer des lignes directrices sur la désinformation et la culture numérique à l'intention des éducateurs.[🔗](#)

Eswatini[🔗](#) et le Soudan[🔗](#) ont coupé l'accès à Internet. La Cour constitutionnelle indonésienne a jugé légal le blocage de l'Internet dans le contexte des troubles sociaux de 2019.[🔗](#)

Le Rwanda[🔗](#) et le Botswana[🔗](#) ont adopté des lois sur la protection des données. Le Sénat brésilien a inclus la protection des données personnelles comme un droit fondamental dans la constitution du pays.[🔗](#)

## Politique des contenus

Microsoft va retirer LinkedIn du marché chinois au motif de l'environnement réglementaire difficile.[🔗](#) Le régulateur chinois entend construire un «internet civilisé» en remodelant le comportement en ligne et en utilisant l'internet pour promouvoir les valeurs socialistes.[🔗](#)

Les recherches de Twitter montrent que ses algorithmes amplifient le contenu de la droite.[🔗](#)

La lanceuse d'alerte de Facebook, Frances Haugen, a témoigné sur les produits et les pratiques de Facebook devant le Congrès américain[🔗](#) et le parlement britannique.[🔗](#) Un consortium de 17 organisations de presse américaines a lancé le projet «Facebook Papers», publiant des documents internes de Facebook obtenus par Haugen.[🔗](#)

Twitter a demandé une législation sur la modération des contenus.[🔗](#) Facebook a exhorté le Congrès américain à mettre à jour la réglementation de l'internet.[🔗](#)

Des législateurs américains[🔗](#) et britanniques[🔗](#) ont interrogé les plateformes de médias sociaux sur la protection des enfants contre les contenus préjudiciables.



en progression

## Questions légales

Un projet de loi portugais visant à donner aux conducteurs de plateformes de VTC des droits en tant qu'employés et non en tant qu'entrepreneurs attend l'approbation du Parlement.[🔗](#)

Google et Facebook se sont entendus pour saper les protections de la vie privée d'Apple.[🔗](#)



en baisse

## Nouvelles technologies (IoT, IA, etc.)

La conférence de la CNUCED15 a conclu que les politiques sont essentielles pour exploiter les technologies d'avant-garde à bon escient.[🔗](#)

Le Parlement européen a appelé à l'interdiction de la reconnaissance faciale dans les espaces publics.[🔗](#) Les États-Unis vont élaborer une «déclaration des droits pour un monde alimenté par l'IA».[🔗](#)

La stratégie de l'OTAN en matière d'IA décrit comment l'IA peut être appliquée à la défense et à la sécurité.[🔗](#) L'ONU a lancé l'initiative «AI for Road Safety» pour réduire le nombre de morts et de blessés sur les routes.[🔗](#)

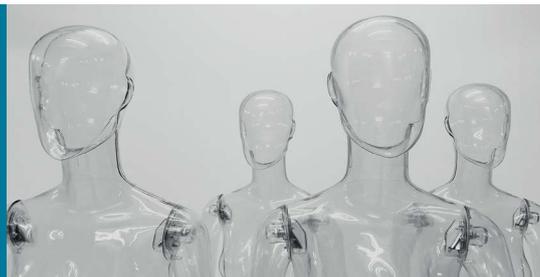
Facebook va embaucher 10 000 personnes dans l'UE pour construire son métaverse.[🔗](#) Pour en savoir plus sur ce concept, voir page 10.[🔗](#)



en progression

## #ICYMI:

Le rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression a présenté son rapport[🔗](#) à l'Assemblée générale des Nations unies, appelant à des efforts plus soutenus pour combler le fossé numérique entre les sexes et faire en sorte que les espaces numériques soient sûrs pour les femmes et les personnes non binaires.



## La troisième fois sera-t-elle la bonne ?

**Les discussions sur les transferts de données personnelles entre l'UE et les États-Unis ont lieu pour la troisième fois. Les deux pays reconnaissent l'importance de réussir à trouver un accord - pour leurs relations bilatérales et pour se positionner en tant que leaders mondiaux en matière de politique numérique. Nous examinons les défis à relever pour parvenir à un accord viable.**

Depuis des années, les États-Unis et l'Union européenne tentent de mettre en place un mécanisme permettant de transférer les données personnelles des citoyens européens vers les États-Unis et de satisfaire aux exigences de la législation européenne en matière de protection de la vie privée. Le premier cadre, Safe Harbor, a été invalidé par la Cour de justice de l'Union européenne (CJUE) en 2015 dans l'affaire dite Schrems I [\[1\]](#). Le second cadre, le bouclier de protection de la vie privée UE-États-Unis, a été invalidé en juillet 2020 dans l'affaire dite Schrems II [\[2\]](#) et ce, sans période de transition, prenant effet immédiatement.

Les raisons de l'invalidation du Safe Harbor et du Privacy Shield sont étonnamment similaires et sont au cœur des négociations en cours entre les deux blocs. Compte tenu des différentes approches en matière de réglementation de la protection des données dans l'UE et aux États-Unis - qui sont littéralement séparés par un océan - de telles négociations sont tout sauf simples. L'UE adopte une approche réglementaire stricte, avec le règlement général sur la protection des données (RGPD) comme principal vecteur de la protection des données personnelles. Les États-Unis adoptent une approche sectorielle de la réglementation de la protection de la vie privée et ne maintiennent pas une loi unique et complète sur la protection des données qui réglemente le traitement des données personnelles au niveau fédéral.

Le principal problème est que pour que les données personnelles des citoyens de l'UE puissent circuler vers les États-Unis sans garanties supplémentaires, les États-Unis sont tenus de fournir un niveau de protection des données personnelles équivalent à celui fixé par le RGPD de l'UE. Ces flux ont des impacts importants sur le commerce et le développement de technologies telles que le *cloud computing* et l'IA.

Plus précisément, le nouvel accord sur le transfert de données personnelles de l'UE vers les États-Unis doit se pencher sur la portée de la surveillance américaine et la mise en place d'un nouveau mécanisme de recours.

### Limiter la portée de la surveillance américaine

Selon la CJUE, l'article 702 de la loi américaine sur la surveillance du renseignement étranger (Foreign Intelligence Surveillance Act) [\[3\]](#), qui permet au gouvernement américain de mener une surveillance ciblée des personnes étrangères situées en dehors des États-Unis et le décret américain 12333 [\[4\]](#) concernant les autorités de surveillance de la communauté du renseignement américaine,

ne satisfont pas aux exigences fixées par l'UE. La réglementation de l'UE exige que les données soient collectées et traitées à des fins spécifiques et justifiables en utilisant des méthodes qui ne portent pas atteinte de manière disproportionnée aux droits fondamentaux de l'homme (principes de nécessité et de proportionnalité).

### Mise en place d'un nouveau mécanisme de recours

La CJUE a également décidé qu'il n'existe pas de mécanisme de recours pour les citoyens de l'UE aux États-Unis. Les citoyens de l'UE devraient être en mesure de savoir si les agences américaines ont collecté ou traité leurs données et d'introduire des recours devant les tribunaux américains si leurs données ont été collectées ou traitées d'une manière qui viole les principes de nécessité et de proportionnalité. L'effort précédent de création d'un médiateur du bouclier de protection de la vie privée [\[5\]](#) au Département d'État américain n'a pas été jugé suffisant.

### Solutions potentielles

En août 2020 - juste après l'arrêt Schrems II - le ministère américain du commerce et la Commission européenne ont annoncé qu'ils avaient entamé des discussions sur un cadre amélioré de bouclier de protection de la vie privée UE-États-Unis. En mars 2021, le service de recherche du Congrès américain a publié un rapport [\[6\]](#) qui résumait les solutions potentielles telles que :

- Un décret limitant la collecte massive de renseignements et prévoyant des mécanismes de recours supplémentaires.
- Un accord diplomatique pour un nouveau cadre remplaçant le Privacy Shield ou un traité de transfert de données.
- Une législation qui limite la collecte de renseignements en masse ou crée un recours d'action pour les personnes non américaines en cas de collecte illégale.

Le commissaire européen à la justice Didier Reynders, qui est en charge des négociations du côté de l'UE, a fait des remarques positives [\[7\]](#) sur de nombreuses propositions innovantes qui sont sur la table.

### Navigation en eau calme ou en mer agitée

Le rythme des négociations dépend du nombre de problèmes qui peuvent être résolus par le pouvoir exécutif [\[8\]](#)

américain, ce qui serait plus rapide que de passer par le Congrès. Si le Congrès doit voter des modifications législatives, notamment en ce qui concerne la modification du système judiciaire pour établir un mécanisme de recours adéquat, plus de temps serait nécessaire. Une autre question est de savoir jusqu'où les États-Unis pourraient aller pour satisfaire la décision de justice de l'UE.

L'UE et les États-Unis doivent également tenir compte d'un paysage réglementaire mondial plus complexe et plus mature en matière de protection des données privées depuis qu'ils ont négocié le Privacy Shield. Pas moins de 17 pays - dont la Chine - ont désormais adopté des lois calquées sur le RGPD, le suivi d'Osaka du G20 a été mis en place, et le G7 a renforcé son soutien au principe de «libre circulation des données dans la confiance», ainsi qu'à l'examen et aux conseils permanents des autorités de protection des données dans le monde entier.

Dans les discussions bilatérales, les négociations sur le bouclier de protection de la vie privée amélioré ont ajouté de la complexité aux négociations du Conseil du commerce et de la technologie (TTC). Alors que le groupe de travail 5 du TTC sur la gouvernance des données et les plateformes technologiques a pour mission «d'échanger des informations sur nos approches respectives de la gouvernance des données et des plateformes technologiques, en recherchant la cohérence et l'interopérabilité lorsque cela est possible», les négociations relatives aux transferts de données personnelles ont été explicitement exclues de l'ordre du jour du TTC et se déroulent en parallèle.

Selon Politico, les responsables européens et américains espèrent qu'un accord sur le nouveau Privacy Shield

amélioré sera conclu d'ici la fin 2021. Cela devrait inclure la création d'un contrôle juridique des agences de renseignement américaines par des juges indépendants qui pourraient se prononcer sur la légalité et la proportionnalité de la collecte des données personnelles des citoyens européens. Il reste à voir quelle endurance Max Schrems a encore pour contester ces dispositions et si ce nouveau mécanisme fera face et résistera à l'examen de la CJUE.

Au niveau mondial, un nouveau nuage se profile à l'horizon : la nouvelle loi chinoise sur la protection des informations privées, qui a des effets extraterritoriaux. Elle mettra inévitablement en lumière les mêmes problèmes de protection des données personnelles des citoyens de l'UE que ceux actuellement discutés avec les États-Unis. En outre, la Chine commence à réclamer un système juridique qui crée et définit les droits de propriété des données, permettant ainsi le commerce des données. Le débat sur la propriété des données en Chine indique également que le gouvernement est prêt à aller bien au-delà que la collecte limitée de données des individus et des entreprises, pouvant être utilisées sans grande restriction dans «l'intérêt public», et à exercer un contrôle sur les données personnelles exportées.

Le travail des agences de protection des données sur l'établissement de principes mondiaux pour les transferts de données personnelles est également à prendre en compte. La Global Privacy Assembly, une plateforme regroupant plus de 130 autorités de protection des données et de la vie privée dans le monde, vient de publier ses Principes pour l'accès gouvernemental aux données personnelles détenues par le secteur privé à des fins de sécurité nationale et de sûreté publique, façonnant ainsi le discours mondial en la matière.



# L'initiative internationale de lutte contre les rançongiciels

Des ministres et des représentants de 31 pays et de l'UE se sont réunis virtuellement pour discuter de l'accélération de la coopération internationale dans la lutte contre les rançongiciels.

La première réunion de l'initiative de coalition contre les rançongiciels s'est tenue à la Maison Blanche les 13 et 14 octobre, après son annonce lors de la déclaration du président Joe Biden sur le mois de sensibilisation à la cybersécurité. Le fait qu'elle se tienne moins de deux semaines après l'annonce témoigne soit d'un enthousiasme impressionnant de la part des alliés et des partenaires, soit d'un travail préparatoire de longue haleine pour le sommet, auquel cas c'est l'absence de murmures et de rumeurs sur l'initiative qui est impressionnante.

## Quel a été le sujet de ces discussions ?

L'ordre du jour a été divulgué le premier jour de la réunion par un haut fonctionnaire de l'administration Biden. Les discussions ont été divisées en quatre grands thèmes : la résilience des réseaux, la lutte contre le financement illicite, la perturbation et les autres efforts de répression, et l'engagement diplomatique. Ces discussions étaient présidées respectivement par l'Inde, le Royaume-Uni, l'Australie et l'Allemagne.

## Quels sont les résultats ?

Le constat est sans appel : «il faut un réseau pour combattre un réseau» : Un réseau de pays doit relier les éléments de la diplomatie, d'agences de sécurité, des régulateurs financiers et des infrastructures - d'abord au niveau national, puis au niveau mondial - pour pouvoir lutter avec succès contre les réseaux de rançongiciels.

Les participants ont convenu d'efforts complémentaires pour réduire le risque de rançongiciels.

## Comment les participants ont-ils été choisis ?

Selon Anne Neuberger, assistante adjointe du président et conseillère adjointe à la sécurité nationale pour le cyber et les technologies émergentes, la Maison Blanche a invité les pays qui «ont des échanges de devises virtuelles dans leur pays, ont un CERT de premier plan, ou qui peuvent vraiment apporter des choses dans la lutte lors de la première vague» et peuvent «déterminer où la coopération fonctionne, où une coopération supplémentaire est nécessaire».

## Un aperçu des efforts de mise en réseau convenus lors du sommet

### Résilience :

- (a) Promotion de la « cyber-hygiène »
- (b) Partage d'informations sur les incidents entre les victimes de rançongiciels, les forces de l'ordre et les équipes d'intervention en cas d'urgence.
- (c) Partage des leçons apprises et des meilleures pratiques pour l'élaboration de politiques de lutte contre le paiement de rançons.
- (d) S'engager avec le secteur privé pour promouvoir le partage d'informations sur les incidents.
- (e) Impliquer activement les hauts responsables dans la prise de décision en matière de cybersécurité.

### Lutte contre le financement illicite :

- (a) Veiller à ce que les cadres nationaux de lutte contre le blanchiment d'argent empêchent la mise en place d'un environnement dans lequel les acteurs malveillants peuvent trouver des plateformes pour transférer des produits illicites.
- (b) Renforcer la capacité des autorités nationales à réglementer, superviser, enquêter et prendre des mesures contre l'exploitation des actifs virtuels.
- (c) Améliorer le partage des informations relatives aux rançongiciels en coopérant avec le secteur des actifs virtuels.

### Engagement diplomatique :

- (a) Coordonner une réponse aux États chaque fois qu'ils ne s'attaquent pas aux activités des cybercriminels pour réduire de manière significative les refuges possibles.
- (b) Coordonner le renforcement des capacités en partageant les approches, les ressources et les programmes disponibles, et veiller à ce que le renforcement des capacités complète d'autres efforts de lutte contre les rançongiciels.

### Perturbation et autres efforts de répression :

- (a) Contrer les activités cybercriminelles émanant de leur propre territoire.
- (b) Échanger des informations et fournir l'assistance demandée pour lutter contre les rançongiciels visant les infrastructures et les institutions financières.
- (c) Prendre des mesures nationales contre les acteurs responsables de rançongiciels ciblant les infrastructures critiques.

## Qui n'a pas été invité ?

Il a été souligné qu'il ne s'agissait pas uniquement d'une initiative américaine, mais que c'était le pays qui distribuait les invitations. La Russie n'a pas reçu d'invitation, ce qui n'a surpris personne et a pourtant fait l'objet d'une certaine couverture médiatique.

Les responsables américains ont expliqué à plusieurs reprises [ici](#) au cours des jours qui ont suivi le sommet que les États-Unis et la Russie discutent des rançongiciels dans un format bilatéral depuis le sommet Biden-Poutine de Genève en juin. Les responsables russes ont toujours souligné que les États-Unis mettaient trop l'accent sur les rançongiciels lors de ces discussions bilatérales [ici](#) et que d'autres sujets tels que les infrastructures critiques et l'ingérence dans les élections devaient également être abordés.

Les États-Unis, quant à eux, pourraient considérer la Russie comme un partenaire peu fiable dans la lutte contre les rançongiciels : le gouvernement russe a pris «certaines mesures» concernant les données sur la cybercriminalité

*Pour en savoir plus sur les cyber-discussions entre les États-Unis et la Russie, consultez le baromètre mensuel de la cyberdétente, [ici](#) publié le 16 de chaque mois.*

partagées bilatéralement par les États-Unis, mais des actions de suivi sont nécessaires.

Mais la Russie n'est pas exclue des futurs événements, pas plus que tout autre pays que les États-Unis n'ont pas invité cette fois-ci.

## L'avenir de l'initiative

Ce sommet, selon un haut fonctionnaire de la Maison Blanche [ici](#), n'était que le premier d'une longue série ; les États-Unis prévoient d'inviter d'autres pays à participer. Toutefois, il a été déclaré que l'implication d'un trop grand nombre de pays pourrait ne pas être propice à l'obtention de résultats concrets. Il sera intéressant de voir à quel moment les États-Unis cesseront d'inviter de nouveaux participants.

Il est également intéressant de noter que 20 des 31 participants sont des signataires et 8 autres des observateurs de la Convention de Budapest sur la cybercriminalité [ici](#), les exceptions étant l'Inde, la Lituanie, la Corée du Sud et les Émirats arabes unis. Cela nous amène à nous demander si cette nouvelle initiative pourrait se traduire par une position ou un projet commun au sein du Comité ad hoc des Nations unies sur la cybercriminalité [ici](#). Ce comité des Nations unies est chargé de rédiger un nouveau traité sur la cybercriminalité et l'on ne sait pas comment il interagira avec la Convention de Budapest sur la cybercriminalité.

## Participants à la première réunion



Australie



Brésil



Bulgarie



Canada



République tchèque



République dominicaine



Estonie



UE



France



Allemagne



Inde



Irlande



Israël



Italie



Japon



Kenya



Lituanie



Mexique



Pays-Bas



Nouvelle Zélande



Nigeria



Pologne



Corée du Sud



Roumanie



Singapour



Afrique du Sud



Suède



Suisse



Ukraine



Emirats arabes unis



Royaume-Uni



Etats-Unis

# Le nouveau battage médiatique en matière de technologie : le metaverse

**Lorsque Facebook a annoncé qu'il allait changer de marque pour refléter la nouvelle orientation de l'entreprise vers la création du metaverse, le battage médiatique autour de ce concept a atteint un nouveau sommet. Qu'est-ce que le metaverse et quels sont ses défis ?**

## Le metaverse original

Le dernier mot à la mode dans le monde de la technologie existe en fait depuis près de 30 ans. Il trouve son origine dans le roman dystopique *Snow Crash*, écrit par Neal Stephenson en 1992. Voici comment il décrivait l'expérience de ses protagonistes dans le metaverse :

*Donc Hiro n'est pas du tout ici en réalité. Il se trouve dans un univers généré par ordinateur que ce dernier dessine sur ses lunettes et envoie dans ses écouteurs. Dans le jargon, cet endroit imaginaire est connu sous le nom de Metaverse.*

## Attributs du metaverse

Un essai populaire sur le metaverse, rédigé par Matthew Ball, spécialiste du capital-risque, identifie ses principaux attributs. Selon Ball, le metaverse sera :

- Persistant - il se poursuivra indéfiniment.
- Synchrones et en direct
- Sans aucun plafond d'utilisateurs simultanés - tout le monde peut faire partie du metaverse en même temps.
- Une économie entièrement fonctionnelle - les utilisateurs pourront créer, posséder, investir, vendre et être récompensés pour leur travail.
- Une expérience qui s'étend à la fois aux mondes numérique et physique, aux réseaux/expériences privés et publics, et aux plateformes ouvertes et fermées.
- Un lieu doté d'une interopérabilité sans précédent des données, des articles et des actifs numériques, et du contenu.
- Peuplé de contenus et d'expériences créés et exploités par un large éventail de contributeurs.

## La vision du metaverse par les entreprises de premier plan

Mark Zuckerberg, PDG de Facebook, a qualifié le metaverse «d'environnement persistant et synchrone où nous pouvons être ensemble». Le PDG de Nvidia, Jensen Huang, l'a décrit comme «un monde virtuel partagé par un grand nombre de personnes. Le design y est réel. Il a une économie réelle. Vous avez un avatar réel. Cet avatar vous appartient et est vous. Il peut s'agir d'un avatar photo-réel de vous ou d'un personnage. Tim Sweeney, PDG d'Epic Games, l'a caractérisé comme «une sorte de terrain de jeu en ligne où les utilisateurs peuvent rejoindre leurs amis pour jouer à un jeu multijoueur comme Fortnite d'Epic à un moment donné, et regarder un film via Netflix le moment suivant». Pour Roblox, le metaverse est «une plateforme de co-expériences immersives, où les gens peuvent se réunir au sein de millions d'expériences 3D pour apprendre, travailler,

jouer, créer et socialiser». Pour Microsoft, le metaverse est une convergence des mondes physique et numérique.

Si vous avez encore du mal à vous faire une idée, voici un exemple tiré de la culture populaire que vous pouvez utiliser comme cadre de référence : la Matrice.

## Les défis

Les principaux défis technologiques seront l'interopérabilité et les normes. Les entreprises devront adhérer à un ensemble commun de normes pour rendre leurs métaverses interopérables. Facebook et Epic Games se sont déjà prononcés en ce sens.

Le principal problème lié à la création de contenu pourrait être la propriété intellectuelle. Dans certaines juridictions (par exemple aux États-Unis et au Royaume-Uni), les droits de propriété intellectuelle ne peuvent être attribués à l'IA, car les œuvres créées par l'IA ne comportent pas d'élément d'intervention humaine. Si un avatar crée quelque chose dans le métaverse, cette création sera-t-elle attribuée à la personne que l'avatar représente ?

Le métaverse posera également de nombreux problèmes de confidentialité et de sécurité, car les données biométriques et de localisation des utilisateurs, ainsi que leurs informations bancaires, seront accessibles au(x) fournisseur(s) du métaverse.

Les plus grandes questions concernent peut-être notre condition d'êtres humains. À qui faisons-nous confiance pour gérer et gouverner le métaverse – s'agit-il d'entreprises technologiques, ou attendons-nous des pays qu'ils disposent de jumeaux numériques de leurs structures de gouvernance dans le métaverse ? Pourrions-nous être sûrs que l'avatar d'une personne n'a pas été piraté avant d'interagir avec elle ? Pouvons-nous être sûrs qu'il s'agit bien d'un être humain ? Comment prouverons-nous notre propre identité aux autres ?

## Qu'en pensez-vous ?

Allons-nous nous perdre dans le métaverse ? Les personnages de Stephenson se sont rendus dans le métaverse pour échapper à leur monde dystopique ; ferons-nous de même si le métaverse nous offre une expérience plus positive que la réalité ? Le métaverse pourrait-il devenir la version réelle de la machine à expériences de Robert Nozick, où nous choisissons le plaisir dans le monde virtuel plutôt que les défis de la vie dans le monde physique ?

# Actualités de la Francophonie



La lettre d'information en français *Digital Watch* est publiée en collaboration et avec le soutien de l'Organisation internationale de la Francophonie [ici](#) dans le cadre de l'initiative D-CLIC, Formez-vous au numérique avec l'OIF.

## La Francophonie à l'honneur au 4e Congrès mondial de l'INGSA

La Secrétaire générale de la Francophonie, Louise Mushikiwabo et le Directeur de la Francophonie économique et numérique de l'OIF, Henri Monceau, ont pris part au **4e Congrès mondial de l'International network for Government sciences (INGSA)** consacré au conseil scientifique aux gouvernements. Avec pour thématique principale « Réinventer le dialogue entre sciences, politiques et grand public », cet événement s'est tenu sous forme hybride au Palais des congrès de Montréal du 30 août au 2 septembre 2021. [ici](#)

Lors de la journée du 2 septembre consacrée à la Francophonie comme espace de coopération et de solidarité scientifique, mais aussi outil de développement économique, le **rôle des sciences en soutien aux politiques publiques** et l'importance de l'expertise francophone ont été soulignés. Lors de la plénière sur « les parties prenantes et la gouvernance », tout en rappelant la mobilisation des scientifiques francophones au moment de la survenue de la crise de la Covid19, la Secrétaire générale de la Francophonie a formulé le vœu que « la langue française soit beaucoup plus présente sur la toile » et plaide **pour une meilleure découvrabilité et accessibilité des publications et ressources scientifiques en langue française**.

Modéré par le Directeur de la Francophonie économique et numérique de l'OIF, l'atelier « Numérique et intelligence artificielle » a permis aux panélistes d'échanger sur **l'intégration des sciences et du conseil scientifique dans les processus de développement des politiques publiques sur le numérique**. L'encadrement des plateformes numériques ainsi que des technologies comme l'intelligence artificielle a notamment été abordé.

## Pour un futur numérique plus inclusif avec la Francophonie numérique 2022–2026

Le projet de Stratégie de la Francophonie numérique 2022–2026 entre dans sa phase conclusive après les travaux d'un groupe de pilotage et des réunions conjointes de la Commission économique/Groupe de travail sur le

numérique de la Francophonie. Par ailleurs, ce projet de Stratégie a été partagé lors de deux événements francophones, la réunion du Réseau francophone des ministres en charge de l'économie numérique à Cotonou (Bénin) et le MTL Connecte à Montréal (Canada-Québec).

À l'occasion de la **deuxième réunion du Réseau francophone des ministres en charge de l'économie numérique** (Cotonou, 3 septembre 2021) organisée avec le soutien de l'OIF, la Secrétaire générale de la Francophonie a réaffirmé l'engagement de l'Organisation auprès des États et gouvernements membres en évoquant notamment les **trois défis majeurs** qu'entend relever la **Stratégie de la Francophonie numérique 2022–2026**, à savoir les fractures numériques, l'uniformisation linguistique et culturelle de l'espace numérique et l'amplification de risques ou de menaces (atteintes à la cybersécurité, manipulation de l'information, violence en ligne, etc.), pour parvenir à un développement numérique inclusif.

**Les défis et opportunités de la transformation numérique dans l'espace francophone ont également été présentés lors de la 3e édition de MTL Connecte – La semaine numérique de Montréal** (12 au 17 octobre 2021), au cours de l'intervention du Conseiller Innovation et numérique du Cabinet de la Secrétaire générale de la Francophonie, Mohammed Traoré, sur le thème « Catalyser un futur numérique plus inclusif avec la Francophonie numérique 2022–2026 ».

Réunissant cette année dans un format hybride plus de 12000 participants et 300 conférenciers originaires de 80 pays, le MTL Connecte [ici](#) est une manifestation à portée internationale qui démocratise les enjeux et les défis liés à la transformation numérique au niveau technologique, économique, social, culturel et environnemental.

Lors de sa conférence donnée le jour de l'ouverture du MTL Connecte, M. Traoré a rappelé que les défis et opportunités de la transformation numérique, accentués par la crise multisectorielle liée à la COVID-19, interpellent les États et gouvernements ainsi que l'ensemble des acteurs de l'espace francophone pour une transformation numérique plus inclusive. Il s'est ensuite attaché à présenter les principaux enjeux et axes d'intervention prévus dans le cadre de la Stratégie de la Francophonie numérique actualisée (2022–2026), **pour**

## accélérer la transformation numérique comme vecteur de développement humain, social et économique.

Les enjeux de la transformation numérique de l'espace francophone ont également été mis à l'honneur au MTL Connecte à travers notamment une table ronde, organisée par le journal Le Monde, sur le thème « Quels sont les nouveaux possibles pour la Francophonie numérique ».

## Mobilisation francophone à Genève autour du numérique

En amont de la XIIe Conférence ministérielle de l'Organisation mondiale du commerce (OMC) qui se tiendra à Genève du 30 novembre au 3 décembre 2021, l'OIF, à travers sa Représentation permanente auprès des Nations Unies à Genève et à Vienne (RPGV), a planifié différentes activités pour les délégations diplomatiques des pays francophones en lien avec la gouvernance internationale du numérique, en particulier une **session d'information sur l'état des discussions multilatérales et plurilatérales sur le commerce électronique**, organisée le 16 novembre 2021 en partenariat avec la Diplo Foundation, et une journée d'échanges qui examinera différents enjeux numériques d'intérêt pour les opérateurs économiques des pays francophones, organisée fin novembre en partenariat avec le Centre du Commerce international (ITC).

À l'initiative de la RPGV, les modalités pour orienter de la meilleure manière **possible le numérique en faveur du développement et les enjeux d'intelligence artificielle** ont également été abordés lors de l'échange que le **Groupe des Ambassadeurs francophones (GAF)** à Genève a tenu avec le Directeur général de l'OMPI, M. Daren Tang, le 24 septembre dernier. Une discussion similaire se tiendra avec Mme Ngozi Okonjo-Iweala, Directrice générale de l'OMC, le 12 novembre prochain.

Par ailleurs, les missions permanentes du Rwanda, de la Bulgarie et de la Fédération Wallonie-Bruxelles ont été nommées coordinatrices du groupe de travail sur le numérique des Ambassadeurs francophones à Genève lors du dernier renouvellement du Bureau du GAF au mois de septembre dernier.

## Favoriser la place de la langue française dans le numérique

Le plaidoyer sur les enjeux du numérique dans l'espace francophone a également trouvé un écho dans la **conférence virtuelle « Osons le numérique en**

**français** » organisée le 29 septembre 2021 par l'association Francophonie sans frontières, en partenariat avec l'Ambassade du Canada en France. S'interrogeant sur la place et le rôle de la langue française dans le numérique en lien avec le développement, l'économie et l'inclusion, les intervenants ont identifié plusieurs pistes de réflexion et leviers d'actions, dont le renforcement de la **découvrabilité des contenus francophones et l'éducation au numérique**.

## Formation des agents publics francophones à la gouvernance numérique

La gouvernance de l'Internet est de plus en plus prépondérante dans le travail des diplomates et des fonctionnaires publics. Afin de renforcer les compétences des agents publics francophones dans ce domaine, la Diplo Foundation en collaboration et avec le soutien de l'Organisation internationale de la Francophonie dans le cadre de l'initiative D-CLIC, Formez-vous au numérique avec l'OIF, lance un **appel à candidatures** pour un **cycle pilote de formation en ligne sur l'introduction à la gouvernance de l'Internet**. Les candidatures provenant des pays francophones en développement membres de l'OIF sont fortement encouragées.

**Cours en ligne**

**Cycle de formation sur l'introduction  
à la gouvernance de l'Internet**



**DIPLO**



ORGANISATION  
INTERNATIONALE DE  
la francophonie



**D-CLIC**  
FORMEZ-VOUS AU NUMÉRIQUE!

En savoir plus : <https://www.diplomacy.edu/courses/gi-oif/>

## Agenda : principaux événements francophones en novembre

- Sommet « Le numérique au service du développement urbain et la résilience des territoires », Namur (Fédération Wallonie-Bruxelles), 4-6 novembre 2021
- Semaine du numérique « Projection à l'ère Post COVID 19 : enjeux d'une transformation digitale réussie », Bobo-Dioulasso (Burkina Faso), 9-13 novembre 2021
- Séminaire de sensibilisation « Enjeux de la gouvernance numérique dans un monde post-Covid » à destination des délégations des pays membres de l'OIF à Bruxelles (Fédération Wallonie-Bruxelles), 30 novembre 2021

# Mises à jour des politiques de la Genève internationale

De nombreuses discussions politiques ont lieu chaque mois à Genève. Dans cet espace, nous vous informons de tout ce qui s'est passé au cours des dernières semaines. Pour d'autres comptes rendus d'événements, consultez la section Past Events sur *l'Observatoire de veille du GIP*.

## La numérisation au service de la protection de l'environnement [14 octobre 2021](#)

Cette discussion s'inscrit dans le cadre de la série d'événements «Reflections on Digital Future» (Réflexions sur l'avenir numérique), qui examine comment façonner notre avenir numérique tout en garantissant le respect et la défense des droits de l'homme. Cet événement a examiné l'impact des nouvelles technologies pour la protection de l'environnement et l'action climatique. Par exemple, l'IA peut renforcer les prévisions climatiques, permettre une prise de décision plus intelligente pour la décarbonisation des industries et anticiper les effets des conditions météorologiques extrêmes. Les panélistes ont posé la question suivante : comment pouvons-nous réellement bénéficier des solutions environnementales offertes par la technologie et utiliser la révolution numérique pour faire progresser la gestion de l'environnement ? Comment

pouvons-nous exploiter de manière appropriée les possibilités offertes par le numérique tout en limitant les effets négatifs de la numérisation sur l'environnement ? Comment pouvons-nous établir des partenariats solides entre les régions pour soutenir une transition numérique qui favorise la protection de l'environnement dans le monde entier ?

Cette série est organisée par la délégation de l'UE auprès des Nations unies à Genève, la mission permanente de la Suisse auprès des Nations unies à Genève, la mission permanente de la Slovénie auprès des Nations unies à Genève (qui assure actuellement la présidence du Conseil de l'UE) et la GIP, en partenariat avec le Centre international de recherche sur l'intelligence artificielle.

## Confiance numérique 2025 [15 octobre 2021](#)

Les panélistes ont abordé la question de savoir comment le manque de confiance numérique se manifeste aujourd'hui et si ce manque de confiance est justifié ou exagéré. La discussion a également porté sur les leçons que l'on peut tirer d'autres secteurs sur la manière

d'instaurer la confiance nécessaire à notre avenir numérique. La conférence a été organisée par le Centre pour l'intégration commerciale et économique de l'Institut universitaire et le Centre pour la confiance numérique de l'EPFL.

## Legal and Governance tour | 12 Tours pour naviguer dans la Genève numérique [28 octobre 2021](#)

L'événement a abordé le fil invisible qui unit l'écosystème numérique : la gouvernance numérique. Les panélistes ont débattu des développements actuels concernant l'envoyé

de l'ONU pour la technologie, l'avenir du Forum sur la gouvernance de l'Internet, la gouvernance de l'IA et d'autres processus qui gravitent autour de Genève.



# Ce qu'il faut surveiller : Événements de politiques numériques mondiales en novembre

Jetons un coup d'œil au calendrier de la politique numérique mondiale. Voici ce qui se déroulera le mois prochain dans le monde entier. Pour encore plus d'événements, visitez la section Events de l'observatoire *Digital Watch*. [🔗](#)

## 11–12 novembre, 2ème Sommet du GPAI (Paris, France) [🔗](#)

Le deuxième sommet annuel du Partenariat mondial sur l'IA (GPAI) présente les résultats des études des dix groupes de travail et jette les bases du développement d'une IA responsable et de l'adoption d'une IA digne de confiance.

## 23–25 novembre, Journées européennes des données ouvertes : Façonner notre avenir avec des données ouvertes (en ligne) [🔗](#)

La toute première édition des Journées européennes des données ouvertes se déroulera en ligne du 23 au 25 novembre sous les auspices de l'Office des publications de l'UE. L'événement vise à présenter la visualisation des données pour le secteur public de l'UE, lorsque neuf équipes de toute l'Europe et d'ailleurs participeront à un Datathon en travaillant sur des applications innovantes basées sur des données ouvertes.

## 29 novembre–3 décembre, European Big Data Value Forum (en ligne et Ljubljana, Slovénie) [🔗](#)

En tant qu'événement associé à la présidence slovène de l'UE, le premier jour du European Big Data Value Forum (EBDVF) 2021 se tiendra à Ljubljana. Le reste de l'EBDVF sera organisé entièrement en ligne, avec de multiples sessions, ateliers, tutoriels et discours non commerciaux. Le thème de cette année est "La transformation numérique alimentée par les données et l'IA".

## 30 novembre–3 décembre, 12e Conférence ministérielle de l'OMC (Genève, Suisse) (en ligne) [🔗](#)

La Conférence ministérielle de l'OMC, à laquelle participent les ministres du commerce et d'autres hauts fonctionnaires des 164 membres de l'organisation, est le plus haut organe de décision de l'OMC. Elle sera co-organisée par le Kazakhstan et présidée par le ministre du commerce et de l'intégration du Kazakhstan, Bakhyt Sultanov.

Novembre

## 22–24 novembre, Forum africain sur la gouvernance de l'Internet (en ligne) [🔗](#)

La 10e réunion du Forum africain sur la gouvernance de l'Internet (AfIGF) se tiendra du 22 au 24 novembre. L'AfIGF rassemble des parties prenantes de tout le continent, telles que des ministres, des responsables politiques et réglementaires, la société civile, l'industrie, etc.

## 29 novembre–1er décembre, Forum des Nations unies sur les entreprises et les droits de l'Homme (en ligne) [🔗](#)

Les principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'Homme fêtent cette année leur 10e anniversaire, qui constituera le thème central du Forum 2021. Cette étape est l'occasion de revenir sur les progrès et les défis réalisés à ce jour et, plus important encore, d'inspirer une nouvelle impulsion en faveur d'une mise en œuvre mondiale à grande échelle par les États et les entreprises au cours de la décennie à venir. Le thème de cette année est "La prochaine décennie des entreprises et des droits de l'Homme : Accroître le rythme et l'ampleur de l'action pour mettre en œuvre les Principes directeurs relatifs aux entreprises et aux droits de l'Homme".

## 30 novembre–2 décembre, Réunion annuelle du GFCE 2021 (en ligne) [🔗](#)

Le Forum mondial sur la cyber-expertise (GFCE) organisera sa réunion annuelle du 30 novembre au 2 décembre et rassemblera plus de 140 membres et partenaires de toutes les régions du monde, dans le but de renforcer les capacités et l'expertise cybernétiques à l'échelle mondiale.

Décembre

### A propos de ce numéro

Numéro 64 de la newsletter *Digital Watch*, publié le 5 novembre 2021 par la Geneva Internet Platform et la DiploFoundation | Contributeurs : Andrijana Gavrilović, Pavlina Ittelson, Marco Lotti, Jana Mišić | Rédaction et conception : Aleksandar Nedeljkov, Viktor Mijatović, et Mina Mudrić | Contact : [digitalwatch@diplomacy.edu](mailto:digitalwatch@diplomacy.edu)

### En couverture :

Facebook face aux critiques. Crédit : Vladimir Veljasević

© DiploFoundation (2021) <https://creativecommons.org/licenses/by-nc-nd/4.0/>

La Geneva Internet Platform est une initiative de

