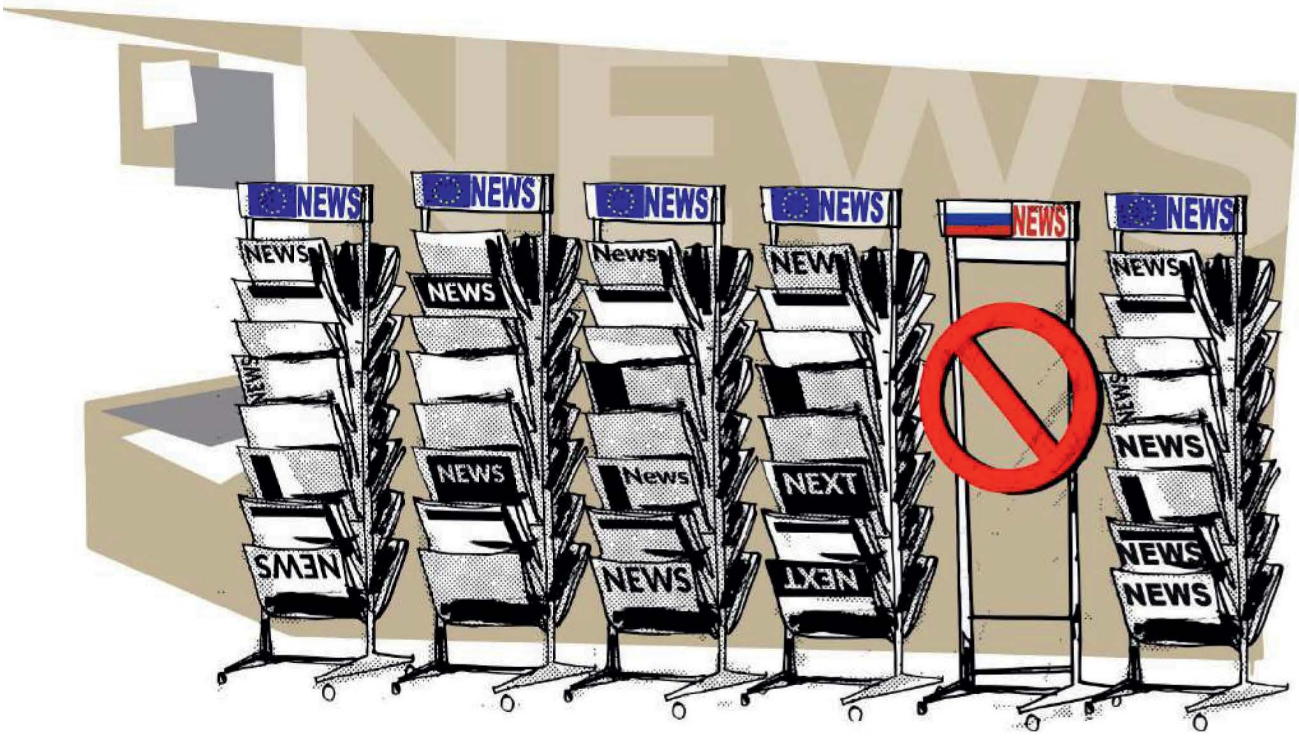
GENEVA INTERNET PLATFORM
digwatch

LETTRE D'INFORMATION

Numéro 68 – Avril 2022



En temps de guerre

Ce qui est autorisé, et ce qui ne l'est pas ? Un rapport spécial sur la guerre en Ukraine

Pages 2–5

MARCHÉ

Le Parlement et le Conseil de l'UE sont parvenus à un accord politique sur la loi sur les marchés numériques, que nous allons analyser.

Pages 6–7

BAROMÈTRE

En dehors du conflit ukrainien, de nombreuses mises à jour ont été effectuées sur les fronts de la sécurité, des infrastructures, de la législation et de la politique de contenu.

Pages 8–9

GENÈVE

Les droits de l'Homme et le commerce électronique occupent une place importante dans l'agenda de Genève en mars. Nous résumons les principaux évènements.

Pages 10–11

À VENIR

Le calendrier des événements de politique mondiale pour avril est assez chargé. Voici les discussions à venir dans notre viseur.

Page 12

ORGANISATION INTERNATIONALE DE la francophonie

D-CLIC FORMEZ-VOUS AU NUMÉRIQUE !

La lettre d'information en français *Digital Watch* est publiée 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.

Bloquer ou ne pas bloquer ?

Alors que la guerre fait rage dans les rues d'Ukraine, la désinformation continue de se propager en ligne, **avec des conséquences néfastes**.

L'un des principaux problèmes est la façon dont la guerre est décrite. La Russie la dépeint comme **une opération militaire spéciale**. L'Ukraine et la plupart des pays ne sont pas d'accord et accusent la Russie de minimiser sa gravité ou de la nier purement et simplement. Ce que l'Occident décrit comme **le massacre de Boutcha** est présenté par la Russie comme **une fausse propagande ukrainienne**.

Certains pays ont pris des mesures énergiques pour freiner la diffusion de la désinformation. **L'UE**, **le Royaume-Uni** et **le Canada** ont interdit aux médias d'État russes *Russia Today* et *Sputnik* d'émettre sur leur territoire (l'agence de presse publique russe TASS n'était pas visée par cette interdiction). La Russie a pris pour cible **la RAI, CNN, CBS, Bloomberg, Euronews** et **Google News**, entre autres.

Un pays – la Suisse – a adopté **une approche différente**. Bien que ces chaînes soient des outils de propagande et de désinformation ciblés par la Fédération de Russie, a expliqué le Conseil fédéral, il est plus efficace de contrer les déclarations fausses et préjudiciables par des faits que de les interdire ».

La décision de la Suisse fait écho à ce que la Fédération européenne des journalistes, la plus grande organisation de journalistes en Europe, **a déclaré en réaction à l'interdiction de l'UE**. « La fermeture totale d'un média ne me semble pas être le meilleur moyen de combattre la désinformation ou la propagande », a déclaré le chef de la FEJ, Ricardo Gutiérrez. Il est toujours préférable de contrer la désinformation des médias propagandistes ou prétendument propagandistes en dénonçant leurs erreurs factuelles ou leur mauvais journalisme ».

Plusieurs problèmes se posent ici. Tout d'abord, aucune de ces approches ne donne les résultats escomptés. L'interdiction des sources médiatiques par le gouvernement permet de freiner la diffusion de la propagande mais impose des limites discutables à l'indépendance des médias et au droit à la liberté d'expression (**même si celui-ci n'est pas absolu**). L'absence de mesures de répression à l'encontre des sources connues de propagande d'État laisse la porte grande ouverte à la diffusion de la désinformation.

Deuxièmement, au-delà de la protection attendue pour les citoyens européens (ou autres), une question plus importante est de savoir à quelles autres sources d'information les citoyens russes ont accès.

Comme l'a fait remarquer Jamie Wiseman, **du bureau de plaidoyer de l'Institut international de la presse**, la Russie a privé ses citoyens de médias étrangers à un moment crucial. Bien que la désinformation doive être contrée par la vérification des faits, **les citoyens russes n'ont tout simplement pas les outils pour le faire depuis le début de la coupure médiatique**. L'appel passionné du Premier ministre britannique Boris Johnson aux citoyens russes, dans leur propre langue, n'atteindra probablement jamais la majorité des citoyens russes.

Troisièmement, attribuer la censure des médias russes à une réaction à l'interdiction de l'UE et d'autres pays (**entre autres des médias d'État**) est discutable. La Russie a certes réagi avec un certain degré de colère, mais elle a décidé de bloquer ou d'étrangler les médias sociaux (et a menacé d'étendre cette mesure aux médias indépendants), **bien avant que d'autres pays** n'imposent leur interdiction aux médias d'État russes.

Le Conseil des droits de l'Homme des Nations unies a fait une avancée la semaine dernière lorsque **le projet de résolution sur la lutte contre la désinformation a été adopté** (sans vote) à la fin de sa 49e session, le 1er avril, **avec très peu de pays se dissociant du texte** (la Russie **a été suspendue de l'organe des droits de l'Homme quelques jours plus tard**).

En fait, il est aujourd'hui largement reconnu que, pour citer la Chine, la désinformation est « un ennemi commun de la communauté internationale ». Les campagnes de désinformation en cours ne disparaîtront pas soudainement, mais les pays comprennent de mieux en mieux ce qui est autorisé et ce qui ne l'est pas, même en temps de guerre.

Russie contre Meta

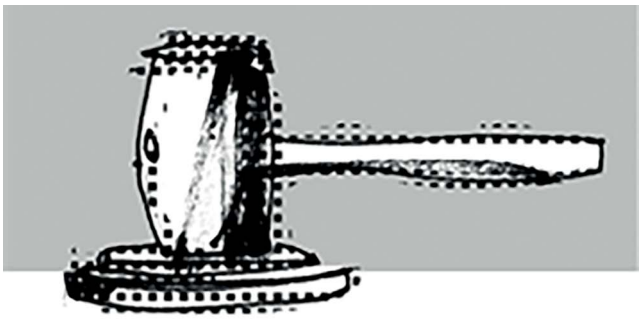
Le discours de haine – ou ce que les textes juridiques appellent souvent l'incitation à la violence – est une problématique très nuancée. Si la désinformation est largement nuisible, de nombreuses nuances du discours de haine sont (généralement) considérées comme illégales.

Ainsi, lorsque Meta a demandé à ses modérateurs de contenu d'autoriser **temporairement les utilisateurs de Facebook et d'Instagram de la région à appeler à la violence contre les soldats russes** le 11 mars, il fallait s'attendre à la réaction de la Russie d'interdire Facebook et Instagram. Même si quelques jours plus tard, Meta a précisé qu'elle proscrivait **les appels à la mort d'un chef d'État** (mais autorisait toujours les appels à la violence), l'interdiction de la Russie **a été confirmée par un tribunal russe**.

Dans un courriel qui a été divulgué à la presse, Meta a informé ses modérateurs qu'il allait accorder une autorisation spéciale validant un certain type de discours violent qui normalement serait supprimé selon la politique interne en vigueur. Cette instruction fait référence aux discours « lorsque : (a) visant des soldats russes, SAUF des prisonniers de guerre, ou (b) visant des Russes lorsqu'il est clair que le contexte est l'invasion russe de l'Ukraine (par exemple, le contenu mentionne l'invasion, la légitime défense, etc) ».

Le texte du courriel de Meta ressemble à une page du code civil ou pénal d'un pays. Pourtant, Meta ne fait pas partie de la branche législative d'un pays et sa politique ne fait pas partie de la loi d'un pays. Cela soulève la question : Devons-nous commencer à considérer les forums de médias sociaux comme des espaces publics, nécessitant des règles normatives applicables par les autorités publiques ? Ou bien doivent-ils continuer à être gérés et contrôlés par des membres du secteur privé, en tant que créateurs de ces espaces ? Ou devrait-on adopter une formule différente qui place ces espaces quelque part entre les deux ? De toute évidence, les gouvernements et l'industrie sont en désaccord.

Les décisions prises en matière de contenu affectent un large éventail de personnes. Dans ce cas, les messages contre les soldats russes d'Arménie, d'Azerbaïdjan, d'Estonie, de Géorgie, de Hongrie, de Lettonie, de Lituanie, de Pologne, de Roumanie, de Russie, de Slovaquie et d'Ukraine seront permis, ce qui affectera à la fois les auteurs et ceux contre qui le discours haineux est dirigé.



Il y a aussi une question de transparence. Les décisions des gestionnaires de contenu de Meta sont basées sur deux choses : les normes communautaires de l'entreprise (la politique) et les directives de l'entreprise sur la façon d'interpréter les normes. La première est une information publique ; **le site Web de Meta comprend un journal des modifications** pour montrer les changements d'une itération des normes à la suivante. Les secondes, les directives de l'entreprise, ne sont pas publiques, mais dans ce cas, elles ont dû être **divulguées à la presse** pour que nous (et le gouvernement russe) en prenions connaissance.

Les lois du pays sont publiques, partout dans le monde. La manière dont la loi est élaborée est également une question publique, conservée dans les archives parlementaires. Il en va de même pour la jurisprudence (à quelques exceptions près).

Si les entreprises veulent continuer (ou regagner la confiance des gouvernements pour persister) à autogérer ces espaces, elles doivent faire davantage pour apaiser les inquiétudes. Bien que certains puissent dire que cela pourrait encourager la transgression, le fait de rendre les directives accessibles au public sur un site web n'incitera pas, en soi, les gens à publier des messages violents.

À elle seule, la transparence ne suffira pas à résoudre les problèmes liés à la politique de contenu. Mais en attendant que les gouvernements et les entreprises y parviennent, les utilisateurs peuvent disposer de repères clairs en cours de route.

L'IA et la reconnaissance faciale en temps de guerre

Lorsque nous avons appris que l'Ukraine utilisait la technologie de reconnaissance faciale Clearview AI (FRT) pour identifier les soldats russes morts, la presse a tiré la sonnette d'alarme. Les critiques disent que l'utilisation de la reconnaissance faciale dans les zones de guerre est un désastre en devenir », **a écrit Thomas Brewster, rédacteur associé de Forbes**.

Le nombre de fois où Clearview AI a été poursuivie devant les tribunaux du monde entier et condamnée à de lourdes amendes pour violation de la vie privée suffit à mettre les gens mal à l'aise, surtout lorsqu'elle est utilisée pendant une guerre.

Pour être clair, la seule utilisation connue de la FRT par le gouvernement ukrainien a été à des fins non guerrières. **Dans une interview**, le vice-premier ministre du pays, Mykhailo Federov, a expliqué que l'Ukraine avait utilisé Clearview AI pour rechercher les comptes de médias sociaux des soldats russes décédés afin de prévenir leurs familles pour qu'elles viennent chercher le corps.

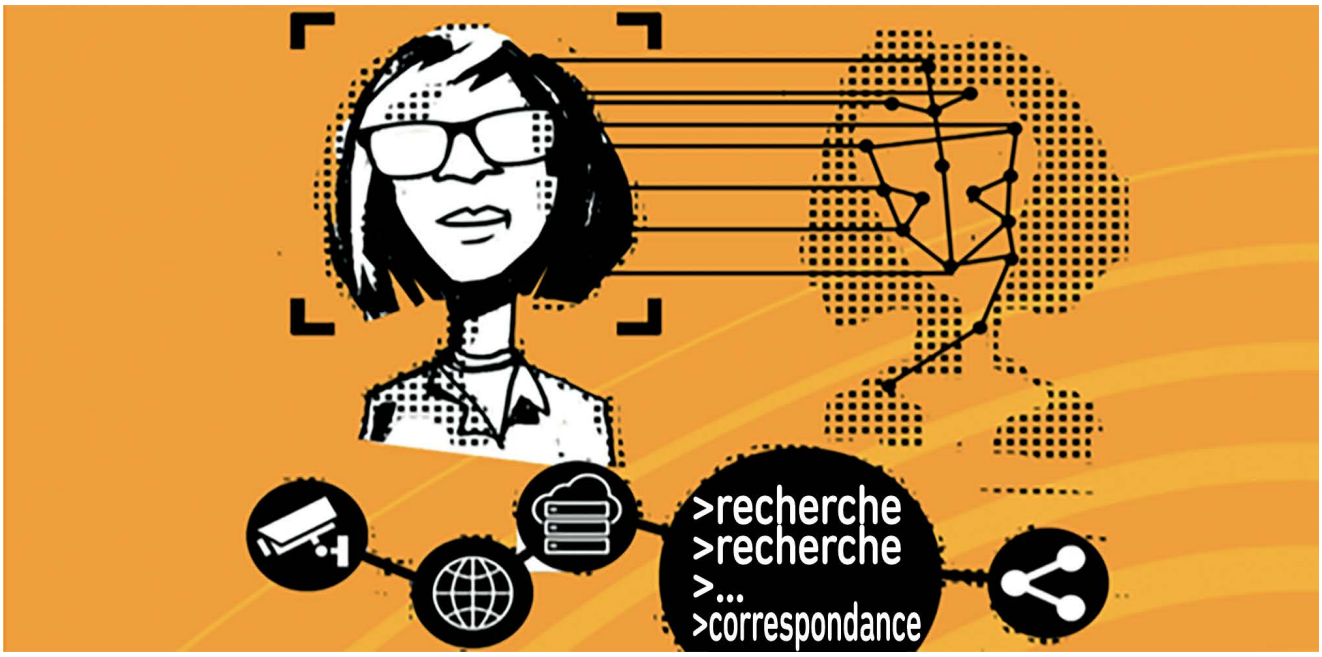
Dans un tweet, Federov a ajouté que le logiciel de reconnaissance faciale « appelle automatiquement les abonnés russes à dire la vérité sur la guerre ». Son tweet faisait référence à « Face ID », vraisemblablement le logiciel de FRT d'Apple, utilisé avec Clearview AI.

La FRT est une arme à double tranchant, car ses erreurs d'identification peuvent induire des conséquences inattendues et dangereuses.

Comme l'a déclaré à Forbes Albert Fox Cahn, fondateur du « Surveillance Technology Oversight Project », « lorsque la reconnaissance faciale fait des erreurs en temps de paix, des personnes sont arrêtées à tort. Lorsque la reconnaissance faciale fait des erreurs dans une zone de guerre, des innocents sont abattus ».

Le problème est donc de savoir ce qui va suivre. Si une partie aux lignes de front, quelle qu'elle soit, commence à utiliser la FRT à des fins allant bien au-delà de l'information des familles russes sur la mort de leurs proches, l'inquiétude augmente de façon exponentielle.

Le taux d'exactitude de l'identification de 99,85 % décrit par Hoan Ton-That, PDG de Clearview AI, ne fait pas grand-chose pour apaiser les craintes concernant les 0,15 % restants. Tout ce qui est inférieur à 100 % peut être désastreux pour quiconque se trouve dans la ligne de mire de la FRT.



Le coût de la cyberguerre pour les autres pays

Bien que l'Ukraine soit l'épicentre de la guerre en cours, d'autres pays sont souvent les dommages collatéraux des cyberattaques visant leurs infrastructures critiques et leurs entreprises.

Par exemple, des représentants de gouvernements européens aidant des réfugiés ukrainiens ont été ciblés par des courriels d'hameçonnage. Ces courriels proviendraient de l'adresse électronique piratée d'un membre de l'armée ukrainienne. La société de cybersécurité Proofpoint a expliqué que **les caractéristiques de cette attaque** sont très similaires aux tactiques employées par **Ghostwriter (ou UNC1151), un groupe de pirates opérant depuis la Biélorussie**.

Au-delà des dommages évidents causés par le logiciel malveillant contenu dans les courriels d'hameçonnage, Proofpoint pense que l'objectif est de répandre un sentiment anti-réfugiés parmi les pays européens et, au final, de diminuer le soutien occidental à l'Ukraine. Cette approche est un **facteur connu** du modèle de guerre hybride employé par l'armée russe et, par extension, par celle de la Biélorussie".

Aux États-Unis, **selon un avis du FBI obtenu par la presse**, le FBI aurait détecté une activité de balayage de réseau provenant de différentes adresses IP basées en Russie, ciblant le secteur énergétique américain. Des entreprises d'autres secteurs, notamment de la défense et des services financiers, ont également été analysées. Les activités de balayage sont courantes, mais le fait qu'elles se soient intensifiées depuis le début du conflit en Ukraine renforce l'idée que l'État russe pourrait être responsable. Le président américain **Joe Biden a également demandé aux chefs d'entreprise de renforcer leur sécurité**. S'adressant à une réunion trimestrielle d'entreprises, Joe Biden a averti que « sur la base de renseignements en constante évolution, la Russie pourrait être en train de planifier une cyber-attaque contre nous... L'ampleur de la capacité cybernétique de la Russie est assez conséquente, et elle est en train d'arriver ».

Le Kremlin a rejeté ces avertissements. Contrairement à de nombreux pays occidentaux, dont les États-Unis, la Russie n'est pas engagée dans le banditisme d'État », **a déclaré le porte-parole du Kremlin aux journalistes**.

Alors, à quoi peut-on s'attendre ? L'histoire récente parle d'elle-même. L'année dernière (avant le début de la guerre), en quelques semaines seulement, une série d'attaques de logiciels malveillants a paralysé les activités du fournisseur américain de **pétrole et de gaz Colonial Pipeline**, de **l'entreprise de production de viande JBS** et du **réseau de santé irlandais. Avec le piratage de SolarWinds, que les États-Unis ont attribué à la Russie**, ces cyberattaques ont été un précurseur des pourparlers américano-russes sur la cybersécurité lancés à Genève en juin 2021 (**aujourd'hui en suspens, peut-être indéfiniment**). Si tout cela s'est produit en temps de paix, le conseil de **CISA de se protéger est à prendre en compte**.

Gardiens de l'Internet, prenez garde : La loi européenne sur les marchés numériques est sur le point d'entrer en vigueur

En début d'année, nous avons récapitulé **conjointement deux projets de loi** – celle sur les services numériques (DSA) et celle sur les marchés numériques (DMA) – qui auront un impact important sur les consommateurs, les entreprises et les grandes entreprises technologiques.

Lorsque nous avons écrit notre article en janvier, le Parlement européen venait d'approuver les textes qui lui serviront de mandat pour négocier avec les gouvernements de l'UE. Après un trilogue intensif de trois mois (**discussions à trois dans le cadre du processus législatif ordinaire**), le 24 mars, le Parlement et le Conseil de l'UE sont parvenus à un accord politique sur le premier de ces textes, la DMA.

Les deux principaux enjeux

Depuis le début du parcours législatif de la DMA, qui a débuté en décembre 2020, les deux plus grandes questions sont :

(a) Quelles entreprises relèveront de la DMA ?

(b) Quelles obligations leur imposera-t-elle?

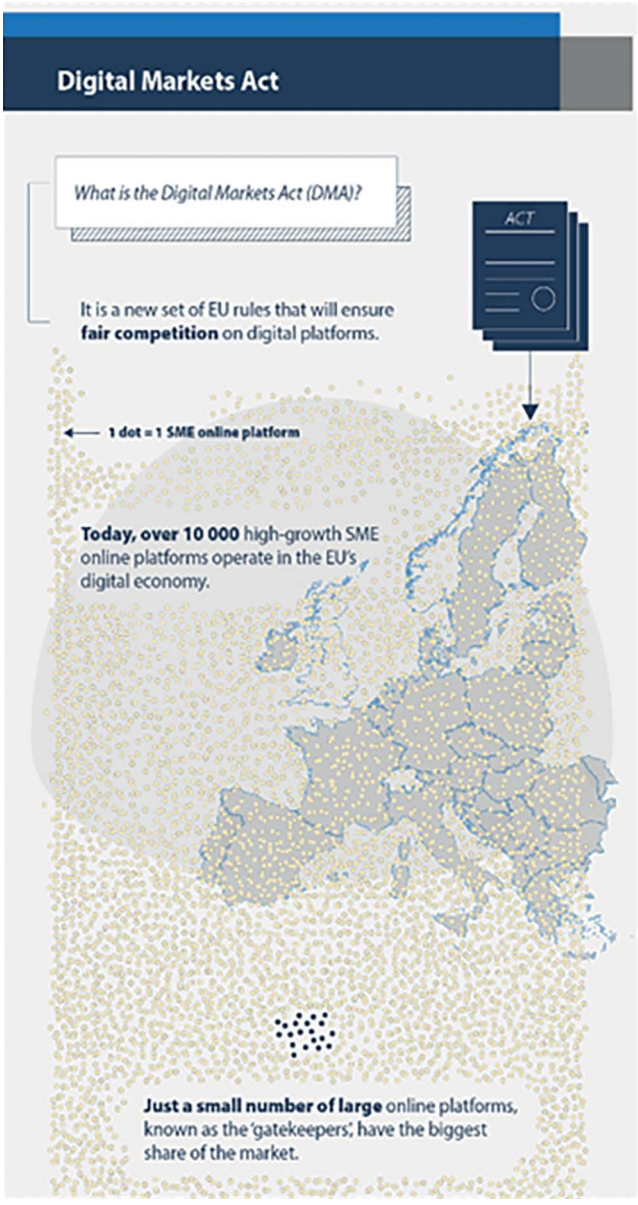
La raison pour laquelle ces deux éléments sont liés est que la loi s'adresse aux entreprises : si vous avez eu suffisamment de succès pour vous retrouver à offrir un service de base aux utilisateurs de l'UE, vous pourriez être désigné comme un « gardien ». Ce titre s'accompagne d'un ensemble d'obligations à respecter.

Qui sont les gardiens potentiels ?

La définition du gardien (au chapitre II du projet de loi) repose sur un ensemble de qualités et de chiffres, que la Commission européenne utilisera pour décider de conférer ou non le statut de gardien à une entreprise.

Premièrement, l'entreprise devra avoir un pouvoir de marché significatif. Tout au long des négociations, l'aiguille avait oscillé entre les entreprises réalisant au moins 6,5 milliards d'euros de chiffre d'affaires dans l'UE (ou une valeur marchande de 65 milliards d'euros), et celles réalisant au moins 8 milliards d'euros de chiffre d'affaires (ou évaluées à 80 milliards d'euros). Finalement, sur la base de ce que le **Conseil de l'UE** et le **Parlement** ont annoncé (aucun texte actualisé n'a été publié), les seuils convenus sont d'au moins 7,5 milliards d'euros de chiffre d'affaires (ou une valeur marchande d'au moins 75 milliards d'euros).

Ensuite, l'entreprise doit également contrôler un ou plusieurs services essentiels, tels que les réseaux sociaux (pensez à Meta), les moteurs de recherche (pensez à



Une section de l'infographie officielle mise à jour sur la loi sur les marchés numériques, qui comprend une représentation visuelle des «gatekeepers» dans le contexte de l'économie numérique de l'UE. Une autre section de l'infographie se trouve à la page suivante. Source : Conseil de l'UE

Google), les places de marché (pensez à Amazon) et les magasins d'applications (pensez à Apple).

On pourrait penser que les législateurs avaient une liste préconçue d'entreprises qu'ils voulaient cibler.

En fait, **les experts disent** qu'ils ont très probablement utilisé le processus dit d'induction à rebours :

La Commission avait une idée approximative des entreprises que la DMA devait prendre en compte, elle a ensuite établi les seuils en conséquence, afin de s'assurer que les grands acteurs seraient inclus.

Les négociateurs auraient eu une liste similaire, y compris des représentants du gouvernement américain **qui ont fait circuler un document politique en huit points parmi les principaux législateurs de l'UE** afin d'éviter de relever les seuils, de peur que la DMA ne cible exclusivement les grandes entreprises technologiques américaines.

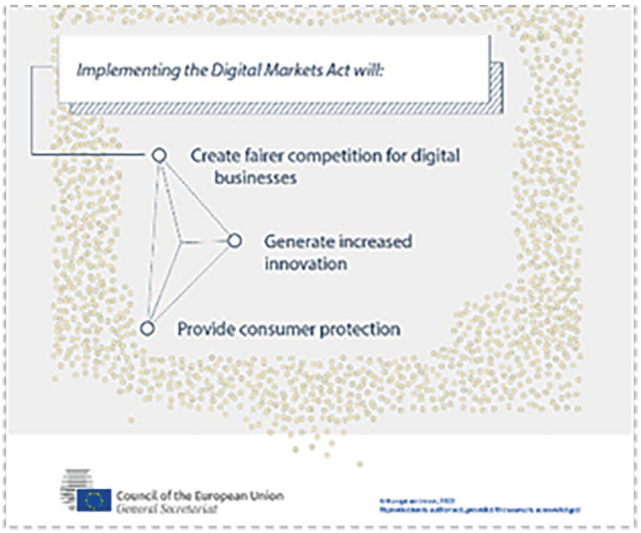
Que se passe-t-il donc si une entreprise veut refuser le titre de « gardien » de la Commission ? Il semble n'y avoir **aucun changement** par rapport à la **version initiale** (voir l'article 4.1) : Une entreprise peut contester la désignation en demandant à la Commission de revoir sa décision.

Quelles sont les obligations imposées par la DMA ?

En l'absence d'un texte juridique actualisé, nous nous baserons sur **le résumé du Conseil de l'UE** :

Les gardiens devront :

- veiller à ce que les utilisateurs aient le droit de se désabonner des services de la plateforme de base dans des conditions similaires à celles de l'abonnement ;
- pour les logiciels les plus importants (par exemple, les navigateurs web), ne pas exiger de logiciel spécifique par défaut lors de l'installation du système d'exploitation ;
- garantir l'interopérabilité des fonctionnalités de base de leurs services de messagerie instantanée avec des services similaires ;
- permettre aux développeurs d'applications d'avoir un accès équitable aux fonctionnalités supplémentaires des smartphones (par exemple, la puce NFC) ;
- donner aux vendeurs l'accès à leurs données de performance marketing ou publicitaire sur leur plateforme ;



- informer la Commission européenne de leurs acquisitions et fusions ;

Mais ils ne pourront plus :

- classer leurs propres produits ou services plus haut que ceux des autres (auto-référencement) ;
- réutiliser des données privées collectées lors d'un service aux fins d'un autre service ;
- établir des conditions inéquitables pour les utilisateurs professionnels ;
- pré-installer certaines applications logicielles ;
- exiger des développeurs d'applications qu'ils utilisent certains services (par exemple, des systèmes de paiement ou des fournisseurs d'identité) pour figurer dans les magasins d'applications ;

La non-conformité entraînera de lourdes amendes. Les entreprises peuvent se voir infliger des amendes allant jusqu'à 10 % de leur chiffre d'affaires mondial total (selon **le projet initial, article 26**), et jusqu'à 20 % en cas de récidive (comme le suggère le Parlement).

Que se passe-t-il ensuite ?

La DMA n'est plus très loin d'avoir force de loi. Il ne reste plus qu'à peaufiner les aspects techniques et à obtenir le feu vert final du Parlement et du Conseil de l'UE. Mais ce n'est pas tout pour les entreprises. La DSA, qui aura également un impact important sur les consommateurs, les entreprises et les grandes entreprises technologiques, est également en route. Nous vous en parlerons le moment venu.

Les évolutions de la politique numérique qui ont fait la une

Le paysage de la politique numérique évolue quotidiennement ; voici les principaux développements du mois de mars. Nous les avons décodés en petites mises à jour qui font autorité. Vous trouverez plus de détails dans chaque mise à jour sur le Digital Watch Observatory.

En hausse

Architecture globale

Le comité ad hoc des Nations unies sur la cybercriminalité a adopté une feuille de route décrivant les prochaines étapes des négociations d'un nouveau traité. Le Groupe de travail à composition non limitée (OEWG) de l'ONU sur les développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale a tenu sa deuxième session de fond. ***Visitez la page UN OEWG 2021-2025 pour plus de détails.***

Un groupe d'experts de l'Internet a proposé un ensemble de principes pour les sanctions relatives à la gouvernance de l'infrastructure de l'Internet.

Le Secrétariat de l'ONU a convoqué une réunion de groupe d'experts pour examiner comment le Forum sur la gouvernance de l'Internet peut contribuer à faire progresser la coopération numérique.

Neutre

Développement durable

L'Union internationale des télécommunications (UIT) a lancé une plateforme d'annonces en ligne Partner2Connect et un cadre d'action pour faire progresser la connectivité universelle et la transformation numérique.

L'Arabie saoudite et l'Égypte ont signé un accord de coopération en matière de transformation numérique.

En hausse

Sécurité

Une attaque par déni de service distribué a mis hors service plusieurs sites web gouvernementaux en Israël. Nvidia, Microsoft, Octa et Samsung ont été piratés par le groupe cybercriminel Lapsus$. Des arrestations liées à ces affaires ont été effectuées au Royaume-Uni.

Le projet de loi sur la sécurité en ligne a été présenté au Parlement britannique. Aux États-Unis, une coalition bipartite de procureurs généraux d'État a lancé une enquête sur les effets de TikTok sur le bien-être des enfants. Une Haute Cour britannique a autorisé une action collective en justice contre TikTok concernant le traitement des données des enfants.

Conflit en Ukraine : De nouvelles cyberattaques et vulnérabilités sont exposées (voir notre page « Conflit en Ukraine : aspects numériques et cybernétiques »).

Neutre

Droits numériques

L'autorité irlandaise de protection des données (DPA) a infligé une amende de 17 millions d'euros à Meta pour des violations du GDPR. Le Sri Lanka a adopté une nouvelle loi sur la protection des données. L'Arabie saoudite a reporté l'application de sa nouvelle loi sur la protection des données au 17 mars 2023.

En hausse

Infrastructure

Intel a annoncé **des investissements importants** dans la recherche, le développement et la fabrication de semi-conducteurs dans l'UE. L'industrie des semi-conducteurs figurait également parmi les priorités du président Biden dans **son discours sur l'état de l'Union**.

L'Assemblée mondiale de normalisation des télécommunications a approuvé les mandats des commissions d'études du Secteur de la normalisation des télécommunications de l'UIT pour la période d'études 2022–2024 et a examiné une série de résolutions et de recommandations.

Neutre

Le commerce électronique et l'économie de l'Internet

Le président américain Joe Biden **a demandé aux agences nationales** d'élaborer des réglementations sur les actifs numériques. La Financial Conduct Authority du Royaume-Uni **a demandé aux opérateurs** de distributeurs automatiques de crypto-monnaies de les fermer.

Conflit en Ukraine : De nouvelles sanctions ont affecté le commerce électronique et les échanges commerciaux (**voir notre page « Conflit en Ukraine : aspects numériques et cybernétiques »**).

En hausse

Politique de contenu

Conflit en Ukraine : La Russie a adopté **une nouvelle loi sur la désinformation** prévoyant des sanctions pour la diffusion de fausses nouvelles liées à son « opération militaire » en Ukraine **et a interdit** les réseaux sociaux Facebook et Instagram de Meta en raison d'un changement de politique qui permet aux Ukrainiens d'appeler à la violence contre les soldats russes. **Plus d'informations en pages 2 à 5.**

Conflit en Ukraine : Le Service de sécurité de l'Ukraine a **détruit** cinq fabriques de robots informatiques, affirmant que ces fabriques pratiquaient le sabotage de l'information pour le compte de la Russie.

En hausse

Juridiction et questions juridiques

Les institutions européennes **sont parvenues à un accord** sur la DMA. ***Plus d'informations en pages 6-7.***

L'UE et les États-Unis ont **un accord de principe** sur un cadre **transatlantique de protection des données personnelles**.

En hausse

Nouvelles technologies

Des groupes de la société civile **ont appelé** l'UE à interdire l'IA prédictive dans le maintien de l'ordre et la justice pénale. La commission spéciale du Parlement européen sur l'IA à l'ère numérique **a conclu ses travaux** par une série de recommandations finales. L'Institut national de technologie des États-Unis **a appelé** à une approche socio-technique pour atténuer les préjugés dans l'IA.

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 dans le cadre de l'initiative D-CLIC, Formez-vous au numérique avec l'OIF.

L'OIF publie une étude sur « Crise du Covid-19 et fracture numérique dans l'espace francophone »

Dans le contexte de la crise du Covid-19 et des mesures sanitaires mises en place par les États et gouvernements pour lutter contre la pandémie, l'OIF, à travers sa Direction de la Francophonie économique et numérique, a lancé une étude pour analyser les répercussions sur les économies et sociétés dans l'espace francophone, à travers l'angle de la fracture numérique et de son risque d'amplification entre les pays et au sein des pays.

Une analyse qualitative et quantitative à l'attention des décideurs

Sur la base des constats révélateurs mis en évidence grâce à des analyses empiriques qualitatives et quantitatives utilisant des données réelles issues des secteurs public et privé, l'étude présente, à l'attention des décideurs, un certain nombre de recommandations de politiques à mener pour renforcer l'inclusion et la souveraineté numérique des États, pour une plus grande résilience face aux chocs.

La dimension de la gouvernance du numérique – à l'ère de l'injonction pour une accélération de l'usage des TIC – transparaît tout au long de l'étude dans les résultats obtenus et les recommandations proposées en matière d'infrastructures matérielles et immatérielles, incluant les questions de normes, règles et procédures propres à façonner l'évolution et l'usage d'Internet.

L'étude porte une attention particulière aux pays en développement et parmi eux les pays moins avancés. Toutefois, les recommandations faites relatives à l'amélioration de l'écosystème numérique des pays peuvent s'appliquer à plusieurs égards aux membres développés.

Des préconisations pour renforcer la souveraineté numérique des Etats et gouvernements

L'analyse est décomposée en quatre parties. La première porte sur les conséquences économiques et sociales de la pandémie sur les économies des Etats et gouvernements membres de l'OIF. La seconde s'attache à la mise en évidence du lien qui existe entre le niveau de la numérisation des pays et leur niveau de développement. La troisième partie est consacrée à l'analyse du comportement des entreprises face à la crise du Covid-19 et à leur résilience. La quatrième partie est dédiée aux préconisations pour construire une souveraineté numérique des États et gouvernements.

Quelques résultats saillants de l'étude

La réduction de la fracture numérique passe par la promotion de l'autonomie et de la durabilité en matière de production, collecte, stockage, diffusion, exploitation et valorisation de l'information numérisée, cela au bénéfice des populations.

Il est important que les pays, en particulier ceux en développement et les PMA, puissent être connectés à Internet via des infrastructures telles que des câbles sous-marins et des dorsales terrestres. La dotation en points d'échange Internet (PEI) et centres de données est également nécessaire pour une gestion rapprochée et optimisée des données par les pays, de même que pour garantir une meilleure cyber-sécurité. Aussi, la capacité des pays à accéder à l'énergie est indispensable, notamment pour les pays du Sud. Au-delà des aspects matériels, une dimension immatérielle est également à prendre en compte, telle l'existence d'un environnement réglementaire capable de réguler adéquatement le secteur des télécommunications, de manière à permettre le développement d'un marché à la fois concurrentiel, innovant et créateur d'emplois. La formation et le renforcement des compétences des individus à l'utiliser les outils numériques est aussi une condition indispensable à la réduction de la fracture au sein des pays et entre les pays. En outre, la capacité de financement des investissements dans la transformation numérique des pays est un enjeu considérable à prendre en compte.

Ce sont là seulement certaines des recommandations non exhaustives faites à l'attention des décideurs politiques dans une étude qui alerte, par ses analyses et résultats, sur le risque d'un creusement de la fracture numérique entre le Nord et le Sud, à l'heure de la crise de la Covid-19 et des inégalités de capacité à financer une transformation numérique qui est devenue indispensable pour tous. Les États et gouvernements membres de la Francophonie pourront trouver dans cette étude des éléments de réponse pour une gouvernance numérique solidaire et inclusive qui ne laisse personne au bord de la route.

Une étude présentée en avant-première à Dakar et Genève

Cette étude a été présentée par l'OIF en avant-première à l'occasion de deux événements récents qui se sont déroulés au courant du mois de mars : **la troisième Conférence internationale sur la Francophonie** économique organisée par l'Observatoire de la Francophonie économique (OFE) et une **Conférence sur la numérisation** organisée par l'Institut des Nations unies pour la formation et la recherche (Unitar). Des acteurs importants issus du monde académique, politique, secteur privé, opérateurs directs de la Francophonie et Organisations internationales ont participé aux discussions autour de l'objectif de réduction de la fracture numérique portée par la Francophonie à travers son étude et plus globalement à travers sa stratégie pour la Francophonie numérique (SFN) 2022-2026. Étaient notamment présents le Centre universitaire de Recherche et de Formation aux technologies de l'Internet de l'Université Cheick Anta Diop de Dakar, la Représentation de la Wallonie-Bruxelles, l'Agence universitaire Francophone, GSMA, Smart Africa, Microsoft, la Conférence des Nations Unies pour le commerce et le développement (Cnuced), la Commission économique des Nations Unies pour l'Afrique (CEA) et le Programme des Nations unies pour le développement (Pnud).

Temps fort francophone à venir

19e séminaire de Fratel – 23–24 mai 2022, Brazzaville (Congo)

Avec pour thème « Quels défis pour la sécurité des réseaux de nouvelle génération ? », ce 19e séminaire du Réseau francophone de la régulation des télécommunications (Fratel) se tiendra les 23 et 24 mai 2022 à Brazzaville, en partenariat avec l'Agence de régulation des Postes et des Communications électroniques (ARPCE) de la République du Congo et l'Institut luxembourgeois de régulation (ILR). Une solution technique de participation et d'interaction à distance est prévue pour les personnes ne pouvant prendre part en présentiel à cet évènement international.

En savoir plus : https://www.fratel.org

Mises à jour des politiques de la Genève internationale

De nombreux débats politiques ont lieu chaque mois à Genève. Dans cet espace, nous vous informons de tout ce qui s'est passé ces dernières semaines.

28 février – 1er avril 2022 | 49ème session du Conseil des droits de l'Homme

S'adressant au Conseil au début de la session, le Secrétaire général de l'ONU, Antonio Guterres, **a lancé un avertissement sévère sur la façon dont la technologie numérique est utilisée pour piétiner les droits de l'Homme** « La technologie numérique est le Far West des droits de l'Homme », a prévenu Antonio Guterres, expliquant comment la censure a été normalisée et comment l'IA permet aux algorithmes de faire de la discrimination. **Ses commentaires font écho à un avertissement** similaire qu'il a lancé plus tôt cette année, mais il a ajouté dans son discours au Conseil des droits de l'Homme que « Internet doit être traité comme un bien public mondial ». Antonio Guterres a également fait référence à sa proposition de Pacte numérique mondial, qu'il a formulée dans son rapport de 2021 intitulé **Notre programme commun**, et qui sera abordée lors du Sommet du futur en 2023. Michelle Bachelet, Haut-Commissaire des Nations unies aux droits de l'Homme, **a également mis en garde contre la désinformation qui ronge les sociétés**, et a encouragé les États à prendre des mesures énergiques pour que la technologie numérique fasse progresser les droits partout dans le monde, plutôt que de les affaiblir.

En ce qui concerne les rapports, le dialogue avec la rapporteuse spéciale sur le droit à la vie privée, Ana Brian Nougrères, le 10 mars, a permis de faire la lumière sur son rapport **« Privacy and Personal Data Protection in Ibero-America » : Un pas vers la globalisation** ? Ana Brian Nougrères a expliqué comment le mécanisme de coopération entre la région ibéro-américaine et l'UE, qui se développe depuis deux décennies, peut servir de modèle de collaboration, et peut-être de premier pas vers une harmonisation mondiale des règles de protection de la vie privée et des données personnelles. ***Lisez notre rapport sur cet événement.***

En ce qui concerne les résolutions adoptées à l'issue de la 49e session, **la résolution sur la lutte contre la désinformation** (adoptée sans vote) appelle les États à s'abstenir de diffuser ou d'héberger des campagnes de désinformation, et à veiller à ce que toute réponse à la lutte contre la désinformation soit conforme au droit international des droits de l'Homme. Un débat de haut niveau aura lieu lors de la prochaine session du Conseil des droits de l'Homme en juin-juillet (**plus d'informations en page 3**).

La résolution sur les droits de l'enfant (adoptée sans vote) a chargé le Haut-Commissariat des Nations unies aux droits de l'Homme d'organiser sa réunion annuelle d'une journée sur les droits de l'enfant en 2023 sur le thème « Les droits de l'enfant et l'environnement numérique ».

Le Secrétaire général des Nations Unies, Antonio Guterres, s'adressant à la 49e session du Conseil des droits de l'homme. Source : capture vidéo

17 mars 2022 | Présentation à Genève du rapport spécial de l'UNDP sur la sécurité humaine

Un nouveau rapport de l' UNDP, intitulé **"New Threats to Human Security in the Anthropocene : Demanding Greater Solidarity"**, montre que le sentiment de sécurité des personnes est au plus bas dans presque tous les pays. (Si vous vous demandez ce que signifie le terme « anthropocène », il s'agit d'un concept proposé pour décrire une époque dans laquelle les humains deviennent les principaux moteurs du changement sur notre planète et modifient radicalement la biosphère de la Terre en posant des défis et en menaçant la sécurité humaine).

S'exprimant lors d'une discussion organisée par le Centre de politique de sécurité de Genève (GCSP) et le bureau de l'UNDP à Genève, à l'occasion du lancement du rapport à Genève, le directeur du GCSP, l'ambassadeur Thomas Greminger, a souligné qu'une approche globale de la sécurité intégrant la sécurité humaine dans le courant dominant de la politique de sécurité n'a jamais été aussi importante.

Le directeur du Bureau du Rapport sur le développement humain (BRDH) de l'UNDP, Pedro Conceição, a évoqué certaines des conclusions du rapport, qui montrent que plus de six personnes sur sept se sentaient déjà en insécurité pendant la période pré-pandémique. La directrice de l'UNDP à Genève, Agi Veres, a salué le rapport comme un ajout utile au traditionnel débat mondial sur la sécurité.

Le responsable de la plateforme Internet de Genève et directeur de Diplo, Jovan Kurbalija, a déclaré que l'infrastructure numérique est devenue essentielle pour la société d'aujourd'hui. Après le test de résistance imposé par la COVID-19, l'Internet est à nouveau mis à l'épreuve avec la guerre en Ukraine (plus d'informations en pages 2–5).

Le représentant permanent adjoint de la Tanzanie, Hoyce Temu, a déclaré que le rapport soulignait la nécessité de donner aux femmes une voix plus forte.

La guerre en Ukraine est un coup terrible porté au multilatéralisme, a déclaré le représentant permanent de la Suisse auprès de l'ONU, l'ambassadeur Jürg Lauber. Le rapport de l'UNDP est aussi un appel au renouveau du multilatéralisme et de la coopération internationale. Les personnes, les gouvernements et la société civile peuvent mobiliser des ressources très rapidement. M. Lauber a souligné que : « Nous devons collectivement adopter un même sentiment d'urgence et utiliser la stratégie de la solidarité pour répondre aux menaces interconnectées auxquelles sont confrontés les gens et la planète à l'échelle mondiale ».

21 mars 2022 | Séminaire de haut niveau : Mettre le commerce électronique au service du développement en reliant les points entre eux

La pandémie de COVID-19 a accru l'adoption du commerce électronique dans le monde entier. Cependant, les pays en développement sont confrontés à de nombreux obstacles qui empêchent les entreprises de tirer parti de la transformation numérique.

Cet événement, organisé par la CNUCED, a porté sur les évaluations de l'état de préparation au commerce électronique de la CNUCED et sur la manière dont les pays en développement peuvent utiliser ces évaluations pour améliorer la mise en œuvre de recommandations politiques concrètes.

Selon Didier Chambovey, ambassadeur et représentant permanent de la Suisse auprès de l'OMC, le passage accéléré à l'activité numérique a déclenché un impact transformationnel sur les modèles de production, de consommation et de commerce. M. Chambovey a souligné que « si la connectivité numérique est un outil essentiel pour promouvoir une croissance durable et inclusive, elle a entraîné un développement asymétrique dans le monde entier ».

Rebeca Grynspan, secrétaire générale de la CNUCED, a rendu hommage au rôle de la Suisse en tant que partenaire essentiel du commerce électronique et de l'économie numérique. La Suisse soutient l'assistance de la CNUCED aux Etats membres qui cherchent à construire leur économie numérique ; il est très bénéfique que ces pays puissent bénéficier de la Suisse et de Genève, centres d'excellence en matière de développement numérique.

Ce qu'il faut surveiller : Événements mondiaux sur la politique numérique en avril

Jetons un coup d'œil au calendrier mondial des politiques numériques. Voici ce qui se déroulera dans le monde entier. Pour plus d'événements, visitez la section Événements du Digital Watch Observatory.

11–12 Avril
SEE 10: RIPE NCC Réunion régionale

La réunion régionale du RIPE NCC pour l'Europe du Sud-Est (SEE) 10 sera accueillie par le réseau universitaire et de recherche de Slovénie (ARNES) et le groupe des opérateurs de réseaux slovènes (SiNOG) les 11 et 12 avril à Ljubljana, en Slovénie. Ce forum régional est l'occasion pour les ingénieurs réseau et autres personnels techniques de partager leurs connaissances et leurs expériences, ainsi que d'identifier les domaines de coopération régionale.

12–13 Avril
IAPP Sommet mondial sur la vie privée 2022

Chaque année, l'Association internationale des professionnels de la protection de la vie privée (IAPP) réunit la communauté des professionnels de la protection de la vie privée afin de créer des réseaux, de proposer des opportunités de formation, de discuter des mises à jour critiques des personnalités du secteur et de découvrir de nouvelles solutions et meilleures pratiques. Le sommet de cette année se déroulera en présentiel à Washington, DC, les 12 et 13 avril. Les sujets abordés comprennent les transferts internationaux de données, la gestion des opérations de protection de la vie privée, la publicité en ligne, les violations/pertes de données et les mesures de la protection de la vie privée.

12–14 Avril
#DRIF22 – Forum des droits et de l'inclusion numérique

DRIF22 est une plateforme pour les communautés de pratique africaines autour de la vie privée, de l'Internet abordable, du genre et des TIC, des droits des personnes handicapées et des TIC, de la surveillance de la santé en période de COVID-19, des coupures d'Internet et d'autres thèmes similaires. L'édition de cette année se tiendra en ligne du 12 au 14 avril, après quoi une série de consultations en personne auront lieu dans 17 pays africains.

21 Avril
Sommet de POLITICO sur l'IA et les technologies

La 5e édition du sommet sur l'Intelligence Artificielle et les technologies organisé par POLITICO présentera des discussions spéciales sur des questions concernant des dossiers législatifs clés tels que la loi sur les données et la loi sur les services numériques (DSA), la protection des données, et la meilleure façon d'exploiter le potentiel de l'IA dans des domaines tels que la cybersécurité, les soins de santé et les jeux. Le sommet aura lieu à Bruxelles le 21 avril.

25–29 Avril
CNUCED Semaine du commerce électronique

La Conférence des Nations unies sur le commerce et le développement (CNUCED), en collaboration avec « eTrade for all » et d'autres partenaires, organisera sa semaine annuelle du commerce électronique. Cet événement se déroulera à Genève et en ligne du 25 au 29 avril 2022, sous le thème « Données et numérisation pour le développement ». L'accent sera mis sur les données, les flux de données transfrontaliers et le rôle crucial qu'ils jouent dans le développement économique et social. **Nous établirons un rapport sur cet événement, alors restez à l'écoute.**

A propos de ce numéro

A propos de ce numéro : Numéro 68 de la lettre d'information du Digital Watch, publié le 10 avril 2022 par la Geneva Internet Platform et la DiploFoundation, sous une licence CC BY-NC-ND 4.0 | Contributeurs : Stephanie Borg Psaila (auteur principal), Andrijana Gavrilović, Kristina Hojstricova, Jana Misić, Virginia (Ginger) Paque, Sorina Teleanu, Marco Lotti, Cécile Desjours | Conception : Viktor Mijatović | Contact : digitalwatch@diplomacy.edu

Sur la couverture :
En temps de guerre. Credit: Vladimir Veljasević

La Geneva Internet Platform est une initiative de :

GENEVA INTERNET PLATFORM digwatch

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

REPUBLIQUE ET CANTON DE GENEVE

DiPLO www.diplomacy.edu