GENEVA INTERNET PLATFORM
digwatch
NEWSLETTER

Numéro 62 – Septembre 2021

La prise de pouvoir numérique des talibans

SÉCURITÉ DES ENFANTS

Les plans d'Apple pour protéger les enfants contre les abus en ligne sont déjà en suspens. Le prix à payer pour les nouvelles mesures est-il trop élevé ?

Page 2

ANTITRUST

Les gouvernements continuent de poursuivre les grandes entreprises technologiques devant la justice. Notre nouvelle base de données revient sur ces développements.

Pages 6–7

VIE PRIVÉE

La Chine fait des efforts en matière de protection de la vie privée. Nous comparons la nouvelle loi chinoise sur la protection de la vie privée avec le RGPD de l'UE (spoiler : les deux sont très similaires).

Pages 8–9

« GIG ECONOMY »

En Californie, la proposition 22, très controversée, a finalement été déclarée inconstitutionnelle. Quelles en sont les principales leçons?

Page 10

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.

L'actualité des politiques numériques : Les talibans sur les réseaux sociaux, la protection des enfants en ligne et le dernier scandale en matière de surveillance

1. Comment faire face aux talibans sur les réseaux sociaux ?

L'Afghanistan a sombré dans le chaos après la prise de contrôle de Kaboul par les talibans. Le groupe militant, autrefois réfractaire à l'internet, est aujourd'hui très au fait de la technologie et utilise les médias sociaux comme un outil de contrôle. Facebook et d'autres plateformes numériques ont fermé des comptes gérés par les talibans ou tenus en leur nom. Twitter surveille les messages de violence.

Mais les entreprises de réseaux sociaux sont confrontées à au moins trois dilemmes majeurs. Le premier est de savoir comment traiter les canaux autrefois utilisés par le gouvernement élu de l'Afghanistan, qui pourraient désormais tomber entièrement entre les mains des talibans. Fermer ces canaux reviendrait à réduire au silence ce qui reste du gouvernement légitime, tandis que ne pas intervenir reviendrait à permettre aux talibans de prendre le contrôle et d'alimenter ces comptes en contenu de propagande.

La deuxième question est de savoir comment empêcher un groupe militant de diffuser de la propagande, même s'il s'agit de contenu qui ne franchit pas le seuil de la violence. Sur les réseaux sociaux, les talibans diffusent en effet une version édulcorée de ce qui se passe en Afghanistan.

Par exemple, les talibans ont partagé des photos et des vidéos de chefs de milice posant avec un dissident connu, qui semblait détendu et à l'aise, afin de démontrer qu'ils traitent les opposants avec respect. Cela contraste fortement avec ce que les agences de presse rapportent, notamment les scènes de violence contre les citoyens et les attaques terroristes en représailles aux forces américaines encore présentes dans le pays.

La troisième question est de savoir comment protéger les citoyens afghans pour qu'ils ne soient pas ciblés pour ce qu'ils disent sur les réseaux sociaux. La crainte de représailles est très forte, à tel point que les Afghans se sont empressés de supprimer les contenus susceptibles d'attirer l'attention des talibans. Facebook a aidé les utilisateurs afghans à verrouiller leurs comptes. Pour les activistes et les défenseurs des droits de l'homme afghans, la possibilité de rester anonyme deviendra une question de vie ou de mort.

Ce que Facebook et Twitter décideront de faire prochainement pourrait déterminer la réaction des autres plateformes. Il est peut-être temps d'unir les forces et d'envisager une approche commune. Les talibans ne sont pas encore implantés au-delà de Facebook et Twitter, mais ce n'est qu'une question de temps avant qu'ils ne se rapprochent des autres réseaux sociaux grand public.

2. Apple annonce de nouvelles mesures pour protéger les enfants – mais pourquoi sont-elles déjà en suspens ?

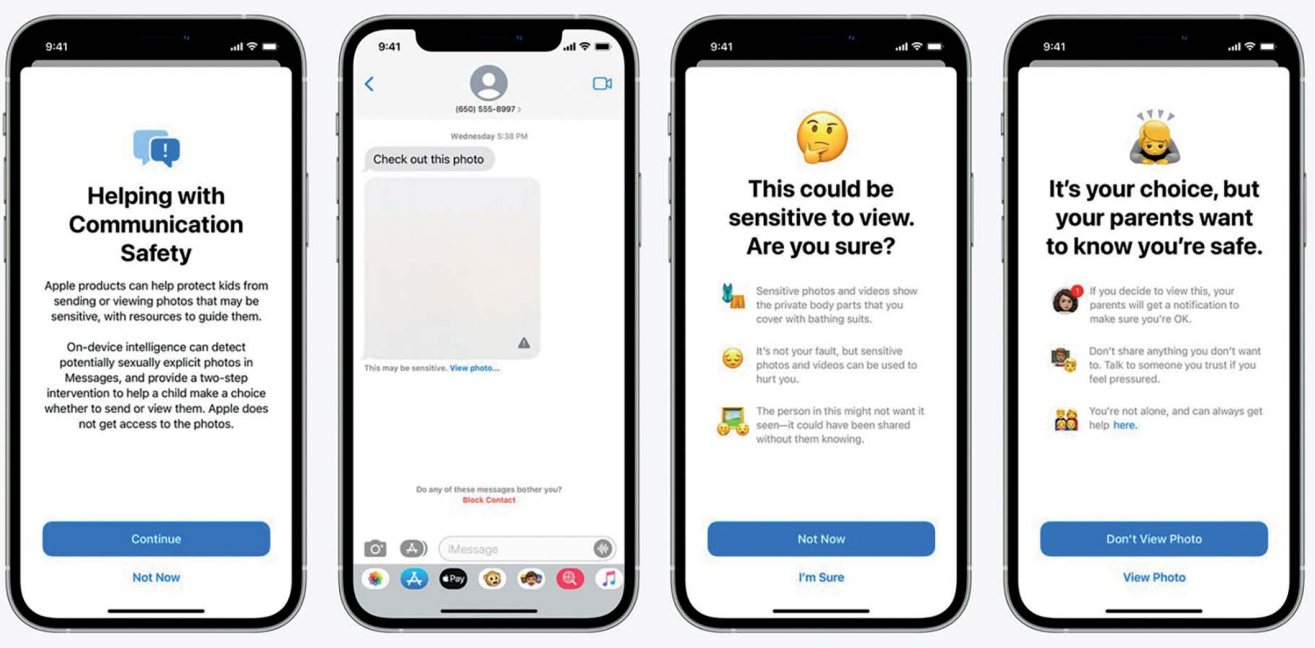
La diffusion de matériel d'abus sexuel d'enfants est un fléau sur internet depuis des décennies. Alors que de nouveaux contenus apparaissent de temps à autre, les photos et vidéos existantes réapparaissent sans cesse, principalement sur le dark web.

Les nouvelles mesures d'Apple, annoncées en août et visant à détecter ces contenus, comportent deux outils principaux : Le premier consiste à détecter de tels contenus sur iCloud Photos, et le second est un ensemble de fonctions de sécurité intégrées à l'application Messages (lisez notre explication de ces outils). Tous deux impliquent une analyse des images directement sur les appareils des utilisateurs.

Le plan initial prévoyait de déployer ces mesures aux États-Unis d'ici la fin de l'année, mais le 3 septembre, Apple a publié la mise à jour suivante : « Sur la base des commentaires des clients, groupes de défense des droits humains, chercheurs et autres personnes, nous avons décidé de prendre plus de temps au cours des prochains mois pour recueillir des informations et apporter des améliorations avant de publier ces fonctions de protection des enfants qui sont d'une importance cruciale ».

En réponse à ces nouvelles mesures, plus de 90 organisations politiques ont signé une lettre ouverte à Apple mettant en garde contre au moins deux problèmes. Le premier est que la capacité d'Apple à analyser les photos iCloud constitue en soi une violation de la vie privée et pourrait « contourner le chiffrement de bout en bout, introduisant ainsi une porte dérobée qui porte atteinte à la vie privée de tous les utilisateurs d'Apple ». La seconde est qu'Apple pourrait être poussé par les gouvernements à utiliser cet outil à leurs propres fins, par exemple à travers l'identification d'autres types de contenu sur les téléphones des utilisateurs.

La réponse d'Apple – qui explique comment l'outil a été conçu dans le respect de la vie privée et ne fournit pas d'informations à Apple sur d'autres photos que celles qui correspondent à des images d'abus sexuel d'enfants connues – n'a pas réussi à apaiser les inquiétudes. Une « porte dérobée reste une porte dérobée », a expliqué le groupe de défense de la vie privée EFF. En termes simples, « Apple prévoit d'intégrer une porte dérobée dans son système de



Messages mettant en garde les enfants contre la réception ou l'envoi de photos sexuellement explicites. Source : Apple

stockage de données et dans son système de messagerie... En fin de compte, même une porte dérobée bien documentée, soigneusement pensée et de portée limitée reste une porte dérobée ».

Le débat sur le chiffrement ne sera pas facile. Apple a depuis promis de revoir les mesures et d'y apporter des améliorations. Si l'entreprise parvient à le faire sans créer de porte dérobée, tout le monde y gagnera, y compris les utilisateurs et les défenseurs des droits de l'homme. Cependant, il est peu probable que les mesures soient aussi efficaces sans une forme de chiffrement réduit.

En définitive, il y a un prix à payer pour assurer la protection des enfants. Dans l'état actuel des choses, le choix aura un prix élevé pour la vie privée des utilisateurs en général, et les mesures révisées auront probablement également un prix à payer. La question est donc : est-ce un prix à payer ?

3. Pegasus : Le dernier scandale de surveillance

La surveillance n'a rien de nouveau. L'homme a toujours été fasciné par l'idée de voir mais de ne pas être vu. Ce que les développements récents montrent, cependant, c'est la privatisation croissante de la surveillance, à travers laquelle des entreprises s'enrichissent à travers la vente de produits d'espionnage.

En juillet, une base de données de personnes considérées comme des cibles potentielles par les opérateurs de l'outil d'espionnage Pegasus a été divulguée à Forbidden Stories, une organisation basée en France. Le président français Emmanuel Macron figurait, entre autres, sur la liste.

Pegasus est en réalité utilisé depuis 2015. Vendu par la société israélienne NSO Group, l'outil exploite une vulnérabilité dans les logiciels de téléphones et est capable de pénétrer dans les appareils sans qu'un utilisateur n'ait à cliquer sur un quelconque lien pour l'activer.

La tendance croissante à tirer profit de la surveillance amplifie la question de savoir qui en est le responsable. Est-ce la responsabilité des sociétés de logiciels dont les produits présentent des vulnérabilités, ou les utilisateurs qui continuent à utiliser des appareils vulnérables ? Les gouvernements, qui achètent de tels outils pour traquer les criminels, mais qui peuvent en faire mauvais usage pour espionner des journalistes, des personnalités religieuses et des universitaires ? Ou s'agit-il d'entreprises comme NSO Group, qui, en réalité, n'enfreignent aucune loi ?

Cela nous rappelle également l'un des principaux problèmes : Les cadres juridiques existants sont trop fragiles et il n'y a pas de base juridique solide sur laquelle s'appuyer. Une solution urgente consiste donc à introduire ou à renforcer la législation qui rend illégale l'exploitation des vulnérabilités, en particulier à des fins commerciales.

Les gouvernements se rendent compte de l'importance de cette question : Le rapport du Groupe d'experts gouvernementaux de 2021 recommande la mise en place de cadres juridiques « pour protéger contre l'utilisation abusive des vulnérabilités des TIC ».

D'ici là, les personnes ciblées sont à la merci des entreprises, des gouvernements et des sociétés de logiciels.

Les développements des politiques numériques qui ont fait la une

Le paysage de la politique numérique évolue quotidiennement. Voici donc les principaux développements de juillet et août. Nous les avons décodés à travers des brèves faisant autorité. Vous trouverez plus de détails sur chaque mise à jour sur l'observatoire *Digital Watch*.

en progression

Architecture mondiale de la GI

Les États-Unis et la Russie ont donné le coup d'envoi des pourparlers sur les enjeux numériques. Les ministres du numérique du G20 ont convenu d'actions visant à accélérer la transition numérique.

Un appel à candidatures pour le groupe consultatif multipartite du FGI 2022 est en cours.

neutre

Développement durable

Plusieurs départements de l'ONU ont lancé une stratégie pour la transformation numérique du Maintien de la paix de l'ONU. Le Conseil de sécurité de l'ONU a appelé à exploiter les technologies numériques pour protéger les missions pour la paix et les civils.

en progression

Sécurité

Les États-Unis, l'Union européenne, l'OTAN et d'autres pays ont accusé la Chine d'avoir mené une cyberattaque contre les serveurs de Microsoft au début de l'année.

Le président américain Joe Biden a exhorté le secteur privé à intensifier ses efforts en matière de cybersécurité, alors qu'une attaque par rançongiciel contre l'entreprise de logiciels Kaseya a touché des clients dans plus de dix pays.

La Russie a proposé un projet de traité sur la cybercriminalité, et une nouvelle stratégie de sécurité nationale.

Les nouvelles mesures de sécurité pour les enfants d'Apple ont suscité des controverses autour de la vie privée, la liberté d'expression et le chiffrement. *Voir notre analyse dans la section Tendances.*

en progression

Le commerce électronique et l'économie de l'internet

Les ministres des finances du G20 ont entériné l'accord de l'OCDE sur les règles fiscales mondiales.

Un tribunal californien a jugé inconstitutionnelle la Proposition 22, qui permet aux entreprises de classer leurs travailleurs comme des entrepreneurs indépendants.

L'autorité française de la concurrence a infligé à Google une amende de 500 millions d'euros pour ne pas avoir négocié de bonne foi avec les éditeurs de presse. Un groupe de 36 États américains et le district de Columbia ont intenté un procès à Google en lien avec les pratiques des « apps stores ».

Le président américain, M. Biden, a publié un décret sur la concurrence, portant sur la neutralité du réseau, l'antitrust et la collecte de données. La Chine a présenté ses plans pour une réglementation accrue du secteur des technologies.

neutre

Infrastructure

Le Sénat américain a adopté un paquet sur l'infrastructure prévoyant 65 milliards de dollars pour développer la connectivité haut-débit.

Google prévoit de construire deux systèmes de câbles sous-marins reliant le Moyen-Orient à l'Europe du Sud et à l'Asie.

La Chine a révélé des plans pour le déploiement massif de la version 6 du protocole internet (IPv6).

Une bataille juridique entre Afrinic et une société basée aux Seychelles concernant l'utilisation de numéros IP en dehors de l'Afrique risque d'entraver les opérations d'Afrinic.

en progression

Droits numériques

Plus de 50 000 personnes étaient des cibles potentielles du logiciel malveillant de surveillance Pegasus. Les experts des droits de l'homme de l'ONU ont appelé les États à interdire la vente de technologies de surveillance.

Le Conseil des droits de l'homme de l'ONU a adopté deux résolutions sur les droits de l'homme et les technologies numériques : La première charge le HCDH d'étudier les coupures d'Internet dans le monde, tandis que la seconde appelle à un débat d'experts sur les processus de standardisation des nouvelles technologies.

La Chine a adopté sa loi sur la protection des informations personnelles. *Lire notre analyse dans la section juridique.*

Amazon a été condamné à une amende de 746 millions d'euros au Luxembourg pour violation du RGPD.

en progression

Politiques des contenus

Les entreprises de réseaux sociaux sont confrontées à des difficultés pour répondre à la présence de contenus liés aux talibans sur leurs plateformes. *Lire notre analyse dans la section Tendances.*

L'ancien président américain Donald Trump a intenté un procès à Facebook, Twitter et Google pour censure présumée.

Un tribunal russe a infligé une amende à Google pour ne pas avoir supprimé des contenus jugés illégaux. Un tribunal pakistanais a révoqué une interdiction de TikTok.

en baisse

Questions juridiques

La Cour suprême d'Autriche demande à la Cour de justice de l'UE (CJUE) d'examiner la légalité de l'utilisation par Facebook des données de tous les utilisateurs de l'UE.

L'avocat général de la CJUE a fait valoir que l'article 17 de la directive européenne sur le droit d'auteur est compatible avec la liberté d'expression.

neutre

Nouvelles technologies (IdO, IA, etc.)

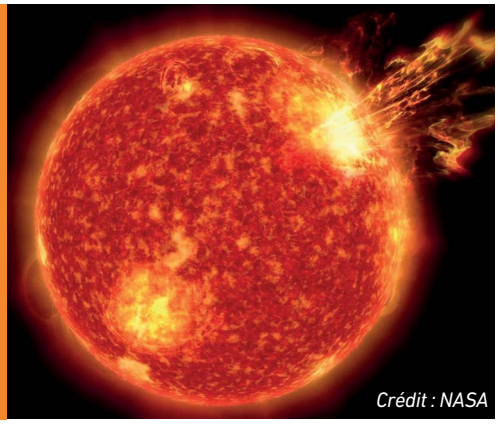
Les États membres neutres de l'UNESCO se sont mis d'accord sur un projet de lignes directrices sur l'éthique de l'IA. L'Irlande et la Turquie ont lancé des stratégies nationales sur l'IA. L'Afrique du Sud et l'Australie reconnaissent que les inventions créées par l'IA peuvent être brevetées.

La Cour suprême de Chine a publié des règles pour réglementer l'utilisation de la technologie de reconnaissance faciale par le secteur privé. L'administration chinoise sur le cyberespace a également proposé des réglementations concernant les algorithmes de recommandation. *Lire notre section Focus pour une analyse.*

#ICYMI

Une nouvelle étude met en garde contre les câbles sous-marins qui pourraient être hors service pendant des mois.

Des phénomènes météorologiques catastrophiques peuvent se produire non seulement sur terre, mais aussi dans l'espace. Lorsque cela se produit (environ tous les siècles), le magnétisme d'une tempête solaire pourrait affecter les câbles sous-marins, entraînant une coupure de l'internet, selon une nouvelle étude présentée lors de la conférence SIGCOMM 2021 sur la communication de données.
« Notre infrastructure n'est pas préparée à un événement solaire à grande échelle », conclut l'étude.



Crédit : NASA

Big Tech: confiance ou concurrence?

Il existe deux armes principales dans l'arsenal des gouvernements pour freiner le pouvoir des géants de la technologie (Big Tech) : les poursuites judiciaires et la législation. Les deux ont été de plus en plus mobilisées ces derniers mois.

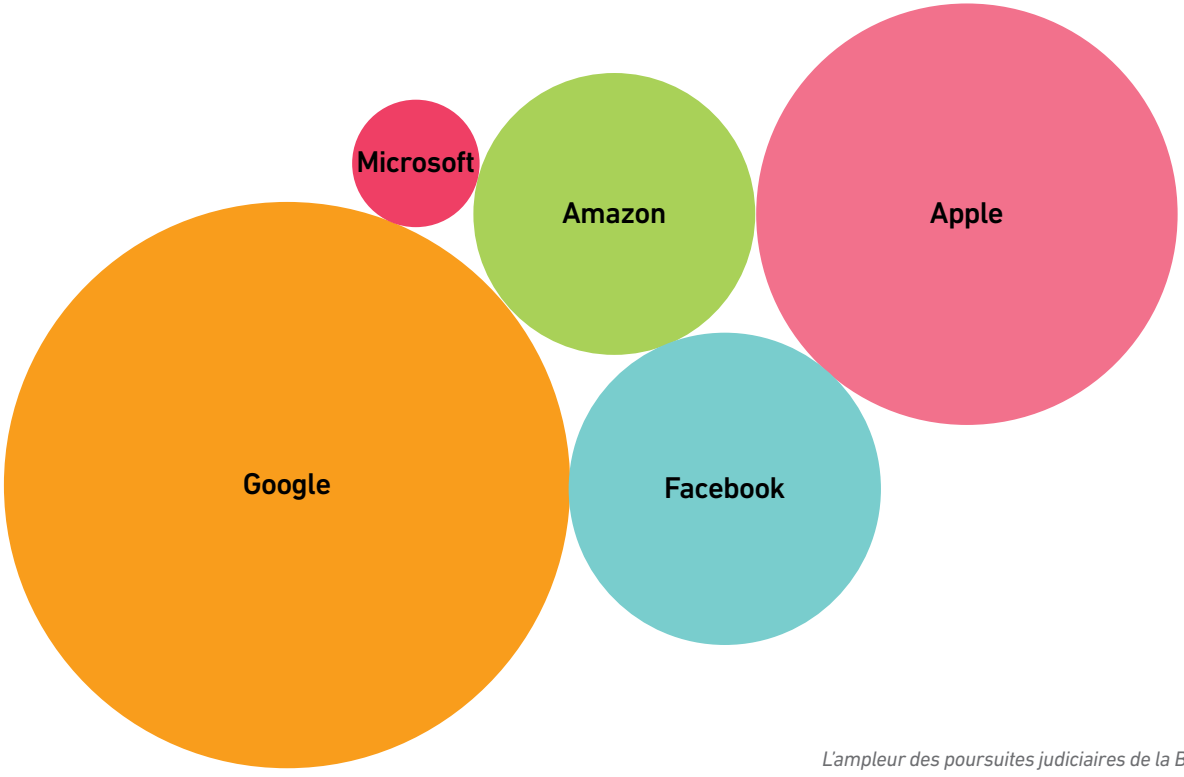
Cette année restera dans l'histoire pour bien des raisons. En matière de politique numérique, il s'agit du pic du nombre d'enquêtes et de procès lancés contre la Big Tech, et plus particulièrement contre Google, Apple, Facebook et Amazon (connus sous le nom de GAFA). Ces affaires surviennent à un moment où les revenus de ces entreprises sont plus importants que le PIB de nombreux pays réunis.

Notre nouvelle base de données interactive des affaires antitrust dans le monde confirme le nombre considérable de nouvelles affaires ayant été introduites cette année, et la concentration de ces cas aux États-Unis et en Europe (et il s'agit surtout de Bruxelles, siège de la Commission européenne). Cependant, des signes clairs montrent que la bataille antitrust s'étend à d'autres pays, avec des enquêtes lancées en Australie, en Inde, en Israël, en Russie et en Turquie.

Les principales préoccupations des gouvernements ont été résumées très clairement (nous ne dirons pas succinctement) dans le rapport de l'année dernière de la sous-commission antitrust de la Chambre des représentants des États-Unis. Les GAFA contrôlent l'accès aux marchés sur lesquels ils opèrent : pour Google, il s'agit de la recherche générale en ligne et de la publicité pour les recherches ; pour Apple, ce sont les systèmes d'exploitation mobiles ; pour Facebook, les réseaux sociaux ; et pour Amazon, la vente au détail en ligne. En outre, ces entreprises essaient de rester au sommet (et d'étendre leur pouvoir sur le marché) en surveillant les autres entreprises pour identifier leurs rivaux potentiels, et en rachetant, copiant ou éliminant leurs menaces concurrentielles.

Les PDG des GAFA peuvent bien avoir des opinions différentes mais partagées sur le nombre d'emplois qu'ils créent et sur leur contribution à l'économie, mais les législateurs américains avaient un message clair : « Le résultat final est moins d'innovation, moins de choix pour les consommateurs et une démocratie affaiblie ». C'est un sentiment qui résonne dans les tribunaux et les parlements du monde entier.

Et pourtant, même si les gouvernements parviennent à maîtriser le pouvoir des GAFA, les critiques ont déjà du mal à croire qu'une nouvelle génération de GAFA ne se lèvera pas à nouveau, en particulier lorsqu'il s'agit de marchés en



L'ampleur des poursuites judiciaires de la Big Tech

pleine croissance comme ceux des jeux vidéos et de la réalité augmentée.

Des changements dans la manière dont Apple et Google gèrent leurs marchés d'applications permettront aux opérateurs historiques de jeux (tels que le créateur de Fortnite, Epic Games) d'atteindre directement des masses d'utilisateurs, sans avoir à passer par les portes de l'App Store ou du Play Store. Ces changements sont désormais imminents.

Les efforts continus visant à limiter le pouvoir des GAFA doivent donc s'accompagner de considérations générales et à long terme sur les nouveaux pouvoirs qui pourraient apparaître à l'avenir. Les poursuites judiciaires et la législation doivent veiller à ce que l'histoire ne se répète pas.

Country/re..	Initiator of ..	Against	Type of case	About	Year initiat..	Year decide..	Status		
							Closed	Decided	Ongoin
Australia	Epic Games	Google	Lawsuit	Epic Games sued Google f..	2021	Pending			✓
China	State Admi..	Alibaba	Investigation	At the end of the 100-day ..	2020	2021		✓	
European Union	Amazon	European C..	Lawsuit	Amazon has filed a lawsui..	2021	Pending			✓
	Epic Games	Apple	Investigation	"The complaint, filed	2021	Pending			✓
	European Commission	Amazon	Antitrust case no 40153	The so-called 'most-favou..	2015	2017		✓	
			Antitrust case no 40462	EC is investigating wheth..	2019	Pending			✓
		Apple	Antitrust case no 40437	EC is investigating Spotif..	2019	Pending			✓
			Antitrust case no 40452	EC is investigating Apple'..	2020	Pending			✓
			Antitrust case no 40652	EC is investigating an e-b..	2020	Pending			✓
			Antitrust case no 40716	EC is investigating compl..	2020	Pending			✓
		Facebook	Investigation	The European Commissio..	2021	Pending			✓
		Google	Antitrust case no 39740	The case was on unfair ad..	2010	2017		✓	
			Antitrust case no 40099	The case alleged that Goo..	2015	2018		✓	
			Antitrust case no 40411	Google was investigated f..	2016	2019		✓	
			Investigation	The European Commissio..	2021	Pending			✓
				The investigation is	2021	Pending			✓
France	Ministère d..	Google	Investigation	The French competition a..	2019	2021		✓	

Notre base de données des affaires antitrust mondiales montre clairement une concentration des affaires aux États-Unis et en Europe. Voir la version interactive.

La nouvelle loi chinoise sur la protection de la vie privée : Une comparaison avec le RGPD

La Chine a introduit une nouvelle loi sur la protection de la vie privée : La loi sur la protection des informations personnelles (ou *Personal Information Protection Law*, PIPL). Se pose désormais la question suivante : dans quelle mesure cette loi est-elle similaire – ou différente – du règlement général sur la protection des données de l'UE, souvent décrit comme une norme mondiale en matière de protection des données ?

La loi chinoise sur la protection des données personnelles a été adoptée le 20 août par le Comité permanent de la 13e Assemblée nationale populaire et entrera en vigueur le 1er novembre.

Notre analyse confirme que, sur le papier, les deux textes sont similaires, la PIPL imposant une peine maximale légèrement plus lourde. Il sera possible d'en dire plus lorsque la PIPL sera effectivement en vigueur, mais en l'état, voici notre comparaison.

		Le RGPD de l'UE	Le PIPL chinois*
Organisation des lois en chapitres et titres	≈	La manière dont elles sont organisées est étonnamment similaire. Elles commencent toutes deux par des dispositions générales (Ch.1) et des principes de protection des données (Ch.2). Ces derniers sont ensuite suivis par : • Les droits des utilisateurs (Ch. 3 dans le RGPD, Ch.4 dans le PIPL). • Transferts transfrontaliers de données (Ch.5 du RGPD, Ch.3 du PIPL) • Obligations des entités traitant des données (chap. 4 du RGPD, chap. 5 du PIPL) • Rôles et responsabilités des autorités (Ch.6 et 7 du RGPD, Ch.6 du PIPL) • Recours et sanctions (ch. 8 du RGPD, ch. 7 du PIPL) • Circonstances particulières (chap. 9 du RGPD, chap. 2 §3 du PIPL). Le RGPD comporte des dispositions supplémentaires (aux chapitres 10 et 11) relatives au fonctionnement de la loi dans l'UE et à la relation du RGPD avec d'autres/anciennes lois sur la vie privée.	
La portée de la loi	≈	Elles s'étendent toutes deux au-delà de leurs frontières géographiques, pour protéger les citoyens européens et chinois, respectivement, où qu'ils se trouvent.	
Ce que signifient les « données personnelles »	≈	Elles ont toutes deux des définitions très similaires des données personnelles.	
Ce que signifient les « données personnelles sensibles »	≈	Elles sont un peu différentes. Dans le cadre du RGPD, cela inclut : • Les données d'identification biométriques • Les données génétiques • Les données de santé • Les opinions politiques • Les origines raciales ou ethniques • Croyances religieuses ou philosophiques • Vie sexuelle ou orientation sexuelle • L'appartenance syndicale	Dans le cadre du PIPL, bien que la liste soit similaire dans certains cas, elle inclut (et laisse de côté) un certain nombre d'autres types de données sensibles. La liste de la PIPL comprend : • Les données d'identification biométriques • Les comptes financiers • Les données relatives à la santé • Informations sur la localisation des personnes • Données personnelles des mineurs (moins de 14 ans) • Croyances religieuses • Statut de personne spécialement désignée
Ce qui est considéré comme une base légale pour que les entités puissent traiter les données personnelles, et comment le consentement d'un utilisateur doit être recherché.	≈	Les deux lois exigent que le consentement des utilisateurs pour le traitement, et toutes deux disent que le consentement des utilisateurs doit être informé, donné librement, et peut être retiré. En ce qui concerne la base de non-consentement, les deux exigent que des contextes similaires existent pour que les entités puissent traiter les données personnelles (à une exception près) : • Lorsqu'un contrat est en jeu • Lorsque des obligations légales l'exigent • Lorsqu'il est nécessaire de protéger les intérêts vitaux des utilisateurs • Chaque fois que l'intérêt public est en jeu.	
	≈	Le RGPD indique que les entités peuvent également traiter les données sur la base « d'intérêts légitimes », un terme vague qui donne aux entités plus de flexibilité. Par exemple, une entité peut recueillir des données afin d'empêcher des activités frauduleuses.	Le PIPL n'inclut pas les intérêts légitimes comme base valable pour le traitement des données personnelles. Au lieu de cela, elle inclut « d'autres circonstances conformément à la loi », ce qui implique des cas dans lesquels une obligation légale est imposée aux entités.

		Le RGPD de l'UE	Le PIPL chinois*
Droits des utilisateurs	≈	Les deux fournissent aux utilisateurs plus ou moins le même ensemble de droits, y compris le droit à l'information, le droit d'accéder aux données personnelles détenues par les entités et de les corriger, et le droit de faire supprimer leurs données.	
Les entités traitant les données (que nous appelons entités, ou parfois entreprises)	≈	En vertu du RGPD, il existe deux grandes catégories de gestionnaires de données : • Le contrôleur : ceux qui décident quelles données personnelles doivent être collectées et comment elles doivent être traitées. • Processeurs : ceux qui détiennent ou traitent les données personnelles. (Il pourrait très bien s'agir d'une seule et même personne ou entité exerçant les deux fonctions.)	En vertu de la PIPL, il existe également deux catégories : • L'entité de traitement des informations personnelles, qui est plus ou moins équivalente au contrôleur du RGPD. • La partie responsable, qui est l'équivalent du sous-traitant du RGPD.
	≈	À part la terminologie, cependant, les droits et responsabilités de base de ceux qui traitent les données sont similaires.	
Transfert transfrontalier de données personnelles, et transferts dans des situations spécifiques	≈	Les deux lois permettent les transferts transfrontaliers de données personnelles si certaines conditions sont remplies. Par exemple, les deux lois autorisent les transferts fondés sur des accords contractuels formulés par les autorités européennes et chinoises, respectivement, ou sur tout autre accord bilatéral international. Il n'est pas encore clair si les mécanismes de la PIPL seront similaires à ceux permis par le RGPD – tels que les clauses contractuelles types – qui sont assez complets (et complexes). En attendant un mécanisme plus clair qui explique comment la Chine autorisera les transferts en pratique, nous pouvons dire que les deux suivent le même esprit d'autoriser les transferts uniquement s'ils sont en accord avec le fait que les données personnelles de leurs citoyens seront bien protégées une fois qu'elles auront quitté leurs frontières.	
	≈	Le RGPD prévoit quelques dérogations lorsque les conditions que nous avons décrites ci-dessus ne peuvent être remplies. En substance, le RGPD offre autant de voies que possible pour permettre le transfert de données personnelles (tant qu'il existe des garanties adéquates pour protéger les citoyens).	Le PIPL, en revanche, prévoit une situation où les données personnelles devront être stockées au niveau national. Si une entité exploite une infrastructure d'information critique ou traite un grand nombre de données à caractère personnel – dépassant le seuil fixé par l'Administration du cyberespace de la Chine – elle ne peut pas transférer les données. La seule exception est si l'entité passe l'évaluation de sécurité de l'Administration du cyberespace, mais cela suggère que le gouvernement jouera un rôle majeur dans la décision de ce qui peut quitter le pays.
Sanctions	≈	Le RGPD impose une pénalité maximale de 4 % du revenu annuel mondial d'une entreprise	Le PIPL impose une pénalité maximale de 5 % du revenu annuel d'une entreprise. Il n'est pas clair si les revenus sont nationaux ou mondiaux dans ce cas. S'il s'agit des revenus mondiaux d'une entreprise, la PIPL prévoit une sanction plus lourde.

**Note : Nous avons utilisé la traduction de Stanford comme version anglaise du PIPL*

Une victoire pour les travailleurs indépendants californiens : La proposition 22 est jugée anticonstitutionnelle

Lorsque la Proposition 22 de la Californie a été adoptée en novembre 2020, beaucoup ont eu l'impression que les chauffeurs et les coursiers avaient perdu face aux entreprises qui faisaient pression pour obtenir ces nouvelles règles. Mais le vent semble avoir tourné.

La Proposition 22 est une mesure électorale qui a permis aux entreprises de continuer à traiter les travailleurs de la « gig economy » californiens comme des entrepreneurs indépendants, en leur donnant des droits minimaux par rapport à ce à quoi les employés ont droit. La mesure a annulé une loi de l'État de 2019 et une décision de la Cour suprême de l'État de 2018, qui auraient obligé les entreprises à reclasser leurs travailleurs en tant qu'employés.

Ce qui a suivi en l'espace de presque un an est une bataille juridique qui a finalement accordé une victoire aux travailleurs : La Cour supérieure du comté d'Alameda a jugé que la Proposition 22 était inconstitutionnelle.

« L'interdiction d'une législation permettant la négociation collective entre les chauffeurs utilisant des applications ne promeut pas le droit de travailler en tant qu'entrepreneur indépendant, ne protège pas la flexibilité du travail et ne fournit pas de normes minimales de sécurité sur le lieu de travail et de rémunération pour ces travailleurs », a écrit le juge. La Proposition 22 est donc désormais inapplicable.

Réaction des entreprises

Dans une déclaration, la coalition représentant les entreprises de la « gig economy », appelée Protect App-Based Drivers and Services, a indiqué que les entreprises prévoyaient de faire appel. Ce n'est pas une surprise, compte tenu de l'ampleur des investissements en lobbying qu'elles ont consentis avant le vote de la Proposition 22.

En parallèle, une autre mesure se prépare aux États-Unis. En août, la Massachusetts Coalition for Independent Work a déposé une proposition de vote visant à créer une nouvelle catégorie de travailleurs dans le Massachusetts. La coalition, qui comprend Uber, Lyft, DoorDash et Instacart, souhaite que les électeurs décident en 2022 si travailleurs de la « gig economy » doivent être considérés comme des entrepreneurs indépendants. La coalition propose que les travailleurs ne soient pas classés comme des employés, mais qu'ils aient droit à certains avantages limités, comme le salaire minimum.

Restez fidèle aux principes

En février dernier, nous avons écrit sur le caractère indispensable des travailleurs de la « gig economy » depuis l'apparition de la pandémie. Nous citions le livre blanc d'Uber, *A Better Deal*, qui expliquait comment « les chauffeurs ont contribué à transporter en toute sécurité des dizaines de milliers de professionnels de la santé » et comment « les coursiers ont fourni un service de livraison essentiel et une bouée de sauvetage pour les restaurants locaux ». Maintenant que la culture des taxis partagés et des livraisons à domicile s'est installée et est susceptible de rester, il est d'autant plus important que les travailleurs soient bien protégés.

Le secteur privé affirme que la plupart de ses travailleurs préfèrent la flexibilité du travail indépendant, plutôt que d'être liés en tant qu'employés. On dit aux travailleurs qu'ils ne peuvent pas avoir les deux. La meilleure façon pour les décideurs politiques de déterminer ce que veulent les travailleurs est de leur demander directement ou de demander à leurs syndicats, ou au moins de lancer des consultations publiques où les travailleurs peuvent exprimer leurs opinions.

D'ici là, il est encore trop tôt pour déterminer à quoi devrait ressembler la meilleure formule. Dans le monde entier, le patchwork des modèles législatifs est très hétérogène.

Pourtant, que les travailleurs de la « gig economy » recherchent la flexibilité ou la sécurité (ou les deux), leurs conditions de travail doivent correspondre à ce qui est annoncé. Les travailleurs indépendants sont généralement en mesure de fixer leurs propres prix, tandis que les salariés peuvent compter sur des congés payés, des congés maladie et d'autres protections de sécurité sociale. Les travailleurs de la « gig economy » n'ont souvent rien de tout cela.

Toute troisième classification en cours d'élaboration ne devrait pas être un outil permettant aux entreprises d'imposer leurs conditions aux travailleurs, tout en mettant de côté leurs responsabilités en tant qu'employeurs. La maxime « on ne peut pas avoir le beurre et l'argent du beurre » s'applique à tous, et pas seulement aux travailleurs.

Mises à jour des politiques de la Genève internationale

De nombreuses discussions politiques ont lieu chaque mois à Genève. Dans cette section, nous vous informons de tout ce qui s'est passé au cours des dernières semaines. Pour d'autres comptes rendus d'événements, visitez la section Événements passés sur l'observatoire du *GIP Digital Watch*.

Discussions du GGE sur les armes létaux autonomes 3–13 août 2021

La première session du Groupe d'experts gouvernementaux (GGE) 2021 sur les technologies émergentes dans le domaine des systèmes d'armes létaux autonomes (SALA) a examiné les recommandations que les parties ont soumises plus tôt dans l'année en ce qui concerne le cadre normatif existant. La deuxième session devrait avoir lieu du 27 septembre au 1er octobre.

Le dialogue sur les innovations de 2021 : Deepfakes, confiance et sécurité internationale 25 août 2021

La session a examiné la façon dont les médias visuels et textuels générés par des algorithmes sont créés et diffusés, et comment ces matériaux pourraient éroder la confiance et présenter de nouveaux risques pour la sécurité et la stabilité internationales. Les questions de gouvernance concernant les deepfakes et les contre-mesures technologiques ont également été examinées. Les participants ont débattu de la question de savoir si de nouveaux outils multilatéraux et multipartites sont nécessaires pour combler les lacunes en matière de gouvernance.

Le tour de l'intelligence artificielle et de l'internet des objets 30 août 2021

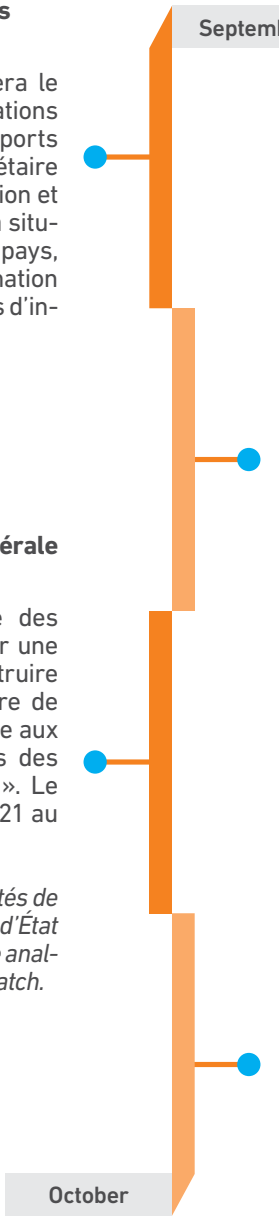
La table ronde, organisée par la Geneva Internet Platform dans le cadre de la série 12 Tours pour naviguer dans la Genève numérique, a expliqué comment Genève rassemble de multiples acteurs travaillant sur l'IA, créant un écosystème unique pour la gouvernance numérique interdisciplinaire et intersectorielle. Les diplomates et les fonctionnaires internationaux devraient profiter des nombreuses opportunités qu'offre Genève en matière de renforcement des capacités sur l'IA et la gouvernance numérique. En outre, malgré les efforts actuels de nombreuses organisations internationales, il est urgent de connecter les incubateurs d'expertise nationaux et internationaux, et de favoriser la coopération sur les applications de l'IA et plus largement sur les technologies numériques.

Ce qu'il faut surveiller : Événements des politiques numériques mondiales en septembre

Jetons un coup d'œil au calendrier des politiques numériques mondiales. Voici ce qui se déroulera le mois prochain dans le monde entier. Pour encore plus d'événements, visitez la section Événements de l'observatoire *Digital Watch*.

13 Sep–1 Oct, 48ème session du Conseil des droits de l'homme (Genève, Suisse)

Le Conseil des droits de l'homme examinera le rapport annuel du Haut-Commissaire des Nations Unies aux droits de l'homme, ainsi que les rapports du Bureau du Haut-Commissaire et du Secrétaire général. Il discutera également de la promotion et de la protection des droits de l'homme, de la situation des droits de l'homme dans plusieurs pays, et de la lutte contre le racisme, la discrimination raciale, la xénophobie et les formes connexes d'intolérance, entre autres sujets.



14–15 Sep, 2ème conférence sur la politique de l'IA (en ligne)

Organisée par RegHorizon et le Center for Law and Economics de l'ETH Zurich, la conférence abordera trois thèmes clés : (a) les implications et les lacunes des propositions réglementaires actuelles et des approches de « soft law » pour les technologies d'IA, (b) la possibilité de nouvelles technologies et d'approches innovantes pour accélérer la préparation des entreprises et assurer une plus grande efficacité de la politique d'IA, et (c) la sensibilisation et l'engagement inclusif des pays du Sud, des jeunes et de la société civile.

14–30 Sep, 76e session de l'Assemblée générale des Nations Unies (New York, États-Unis)

La 76e session de l'Assemblée générale des Nations Unies s'ouvrira le 14 septembre par une réunion de haut niveau sur le thème « Construire la résilience par l'espoir – pour se remettre de COVID-19, reconstruire la durabilité, répondre aux besoins de la planète, respecter les droits des personnes et revitaliser les Nations Unies ». Le débat général sur ce thème se déroulera du 21 au 30 septembre 2021.

Comme d'habitude, nous analyserons les priorités de la politique numérique identifiées par les chefs d'État dans leurs discours lors du débat général. Notre analyse sera disponible sur l'observatoire Digital Watch.

28 Sep–1 Oct, Forum public de l'OMC 2021 (en ligne et à Genève, Suisse)

L'édition 2021 du Forum public de l'OMC a pour thème « Le commerce au-delà de COVID-19 : Construire la Résilience », et examinera comment le système commercial multilatéral peut contribuer à renforcer la résilience face à la crise COVID-19 et aux crises futures. Le forum s'articulera autour de trois sous-thèmes : L'amélioration de la résilience au-delà de COVID-19, le renforcement du système commercial multilatéral, et l'action collective en faveur du commerce durable.

A propos de ce numéro

Numéro 62 de la newsletter *Digital Watch*, publié le 10 septembre 2021 par la Geneva Internet Platform et DiploFoundation | Contributeurs : Stephanie Borg Psaila (rédactrice), Ana Maria Correa, Andrijana Gavrilović, Marco Lotti, Virginia (Ginger) Paque et Sorina Teleanu | Traducteur de l'édition française: Clément Perarnaud | Rédaction et conception : Aleksandar Nedeljkov, Viktor Mijatović, et Mina Mudrić |
Contact : digitalwatch@diplomacy.edu

En couverture

La prise de pouvoir numérique des talibans. Crédit : 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