GENEVA INTERNET PLATFORM
digwatch

NEWSLETTER

Numéro 59 – vendredi 30 avril 2021

En l'IA nous croyons ?

La nouvelle proposition de règlement de l'UE sur l'IA adopte une approche fondée sur le risque. Voici ce que les entreprises, les utilisateurs, les décideurs politiques - et l'UE - doivent savoir.

Pages 2, 10

FUITES DE DONNÉES

Alors que les données de millions d'utilisateurs de Facebook et de LinkedIn se retrouvent entre de mauvaises mains, nous nous penchons sur les problèmes auxquels les régulateurs sont confrontés.

Pages 2, 6

SOLARWINDS

L'attaque SolarWinds, qui a touché au moins neuf agences fédérales américaines et plusieurs pays, a été officiellement attribuée à la Russie par les autorités américaines. La suite des événements est cruciale.

Page 3

SEMI-CONDUCTEURS

L'omniprésence des puces électroniques signifie que la pénurie actuelle a des implications géopolitiques importantes pour les États-Unis, l'Europe, la Chine et Taïwan.

Pages 8-9

ÉVÉNEMENTS MONDIAUX À VENIR

Notre calendrier aide les praticiens de la politique numérique à suivre les principales conférences et réunions mondiales. Jetez un coup d'œil aux événements du mois de mai.

Page 12

Les 3 principales tendances du mois d'avril : Réglementer l'IA, le *scraping* de données et les suites de l'affaire SolarWinds

Chaque mois, nous analysons des centaines de développements en cours afin d'identifier les tendances clés qui ont un impact sur le travail des praticiens de la politique qui travaillent dans ces domaines. Voici ce qui a compté en avril.

1. Réglementation de l'IA

La proposition de règlement de l'UE pourrait devenir une norme mondiale, mais le chemin sera long et les décisions difficiles

L'intérêt des gouvernements pour la réglementation des systèmes d'IA est plus visible que jamais, surtout après la publication, le 21 avril, du projet de proposition tant attendu de l'UE. La proposition adopte une approche réglementaire fondée sur le risque : Si un système présente un risque exceptionnel, il sera interdit ; s'il est considéré comme à haut risque, il sera fortement réglementé ; si le risque est limité, il s'agira alors d'être transparent à son sujet. *Plus d'informations en page 10.*

Selon les experts, il existe une similitude frappante avec le RGPD : Tous deux adoptent une approche globale, ce qui signifie que les règles proposées réglementent toute personne – où qu'elle soit – dont le système est utilisé au sein de l'UE ou touche des citoyens de l'UE. Cette approche normative et cette portée juridictionnelle pourraient aider la proposition à devenir une référence mondiale pour la réglementation de l'IA et le développement des systèmes d'IA.

Mais l'Union européenne ne doit pas se contenter de revendiquer une norme mondiale. Elle devra évaluer l'impact potentiel du nouveau cadre juridique, sous peine de perdre (encore) face aux États-Unis et à la Chine : Une réglementation stricte est susceptible de décourager le secteur privé d'innover et de développer des systèmes d'IA dans l'UE ; mais une approche plus laxiste ne ferait que retarder la recherche de solutions à des questions importantes, y compris éthiques, à un moment où il sera trop tard. Les experts qui traitent des questions de concurrence dans le monde entier ne le savent que trop bien.

Pour l'essentiel, les décideurs et les responsables politiques européens devront se mettre d'accord sur la portée et la profondeur de la réglementation. Ils devront décider quels systèmes sont trop risqués pour la société, lesquels peuvent être tolérés (bien que réglementés) dans l'intérêt de l'innovation, et lesquels doivent être laissés de côté. Ces décisions auront en fin de compte un impact sur le niveau de confiance que la société accordera aux systèmes d'IA et à ceux qui les gèrent, non seulement dans l'UE, mais dans le monde entier.

2. *Scraping* de données

Les dernières fuites de données de Facebook et de LinkedIn s'expliquent par le « scraping » de données, et non par des piratages… il ne s'agit pas seulement de jargon technique

Nous avons l'habitude d'être informés de fuites massives de données. Facebook estime que cette activité se produit – et continuera de se produire – régulièrement.

Cependant, Facebook et LinkedIn ont tous deux répondu ce mois-ci aux violations massives de données – affectant plus de 500 millions d'utilisateurs sur chaque plateforme – d'une manière similaire. Selon ces géants des réseaux sociaux, il ne s'agissait pas d'un piratage, mais plutôt d'un incident de *scraping* de données survenu il y a plusieurs années, les bases de données d'informations personnelles n'étant mises en ligne que maintenant.

À première vue, les deux termes – piratage et *scraping* – évoquent des éléments de méfait technique. Pourtant, ils peuvent tous deux avoir les mêmes conséquences désastreuses : Les données personnelles censées être privées ou protégées sont désormais dans le domaine public et peuvent être exploitées par des acteurs malveillants. Brèche ou pas, les utilisateurs risquent d'être victimes de phishing ou d'autres pratiques frauduleuses, comme cela a déjà été le cas. Ces deux pratiques sont une invitation malvenue à une activité criminelle plus importante, qui est largement réglementée et punie par la loi dans le monde entier.

Cependant, cette pratique révèle des problèmes de société plus profonds et reflète le prix que nous sommes prêts à payer pour davantage de services gratuits, de connexions sociales, ou de produits innovants. En fin de compte, notre volonté – ou la manière dont nous nous y prenons – pour imposer des normes plus strictes aux entreprises est le reflet de la valeur que nous attachons à nos données personnelles et à notre vie privée, ainsi qu'à celles des générations futures.

Les pages 6 et 7 présentent une analyse approfondie des conséquences du scraping de données pour les régulateurs et les utilisateurs.

3. Les suites de l'affaire SolarWinds

L'espionnage a été soigneusement planifié et exécuté – ce qui se passe ensuite est encore plus important

Les États-Unis ont formellement attribué l'attaque SolarWinds de l'année dernière au service de renseignement extérieur russe. Au moins neuf agences fédérales américaines ont été piratées et plusieurs autres pays ont été touchés.

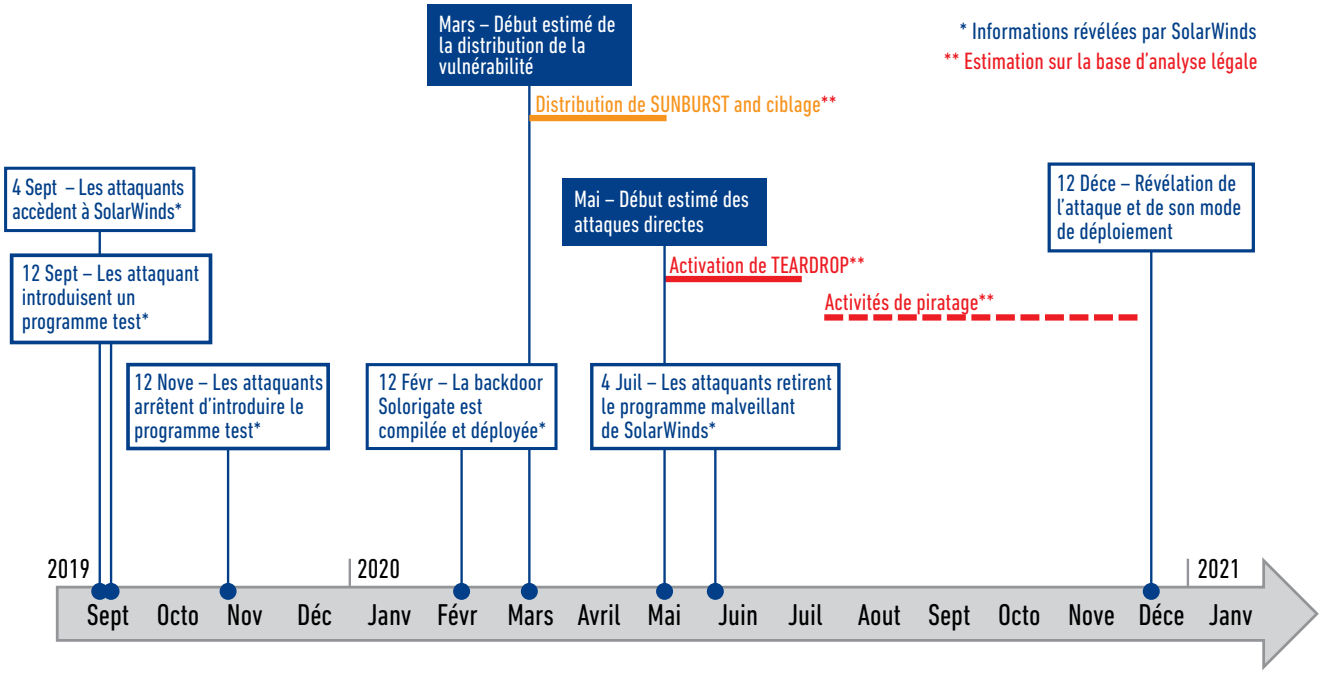
La suite de cette attribution a mené à un échange de menaces et d'actions : dans un décret, le président américain Joe Biden a sanctionné une quarantaine de personnes et entreprises russes, après quoi la Russie a expulsé dix diplomates américains. L'OTAN, l'UE, le Royaume-Uni et l'Australie ont immédiatement exprimé leur soutien en faveur des États-Unis – ce qui montre que l'administration Biden a travaillé en étroite collaboration avec ses alliés pour amplifier le message et montrer un front uni.

La suite des événements sera critique. Bien que l'attaque ait été qualifiée d'espionnage (ce qui signifie que des informations ont été prises, mais que rien n'a été détruit ou perturbé), cela ne signifie pas que les auteurs n'utiliseront pas leurs renseignements nouvellement acquis pour une cyberattaque. En outre, les États-Unis ne savent toujours pas s'ils ont réussi à nettoyer leurs systèmes de l'intrusion.

La principale question est de savoir si les sanctions seront suffisantes pour dissuader la Russie (et d'autres pays) de se livrer à des activités hostiles similaires et si les États-Unis modifieront leurs stratégies de dissuasion et de « défense en avant ». La Maison Blanche a déjà signalé que les sanctions ne représentaient qu'une partie des mesures que les Etats-Unis allaient prendre et que « certains éléments de nos réponses à ces actions resteront invisibles ».

Les États-Unis devront évaluer les implications de leurs réponses et s'assurer qu'ils ne franchissent pas le seuil de ce qui est considéré comme une attaque armée. Bien que la dissuasion puisse être inefficace, les experts ont suggéré que les États-Unis devraient se concentrer davantage sur le renforcement de leurs défenses.

Sur une note plus positive, les experts affirment également que les deux parties ont laissé la porte ouverte au dialogue : M. Biden a déclaré qu'il était temps de désamorcer les tensions par le dialogue et la diplomatie ; la Russie n'a pas rejeté l'idée de M. Biden d'organiser un sommet. L'avenir nous le dira.



Chronologie de l'attaque de SolarWinds (Credit: Microsoft)

Évolution des politiques numériques en avril

Le paysage des politiques numériques évolue quotidiennement. Notre objectif est de faire gagner du temps aux praticiens: nous décodons, contextualisons et analysons les évolutions en cours, en proposant des mises à jour digestes mais faisant autorité. Vous trouverez plus de détails concernant chaque développement sur l'observatoire *GIP Digital Watch*.

neutre

Architecture mondiale de la GI

Les ministres du G7 chargés du numérique et de la technologie ont présenté des plans de coopération sur un large éventail de questions, notamment les chaînes d'approvisionnement, les normes numériques, les flux de données et la sécurité sur internet.

Le groupe d'experts gouvernementaux 2020–2021 sur les systèmes d'armes autonomes létaux a conclu ses travaux.

L'appel à propositions de sessions pour la 16e réunion du Forum sur la gouvernance de l'Internet est ouvert jusqu'au 26 mai.

en baisse

Développement durable

L'Égypte a lancé le projet *Vie décente* visant à connecter 1300 villages à la fibre optique.

Le Bangladesh, le Brésil, la Chine, l'Égypte, l'Inde, l'Indonésie, le Mexique, le Nigeria et le Pakistan ont lancé l'initiative d'apprentissage numérique E9.

La Commission économique pour l'Afrique a créé l'initiative *Apprendre les TIC aux filles*.

en progression

Sécurité

Les États-Unis ont officiellement attribué la cyberattaque de SolarWinds à la Russie et ont imposé des sanctions. *Lire le commentaire en page 3.*

Le Parlement européen a adopté un règlement obligeant les plateformes en ligne à supprimer ou désactiver l'accès aux contenus terroristes dans l'heure qui suit la notification.

Plusieurs institutions de l'UE ont été touchées par un incident de sécurité informatique. Le fournisseur d'Apple Quanta Computer Inc. a été frappé par une attaque de *ransomware*.

en progression

Le commerce électronique et l'économie de l'internet

L'autorité chinoise de la concurrence a infligé une amende de 2,8 milliards de dollars à Alibaba pour pratiques anticoncurrentielles. L'autorité russe de la concurrence a lancé des enquêtes sur Yandex et YouTube. Un rapport du régulateur antitrust australien affirme que des mesures sont nécessaires pour remédier à la domination du marché par les *apps stores* d'Apple et de Google.

Google s'est vu infliger une amende de plus de 36 millions de dollars en Turquie pour avoir abusé de sa position dominante dans les services de moteurs de recherche.

Les États-Unis ont proposé un impôt minimum mondial pour les entreprises, y compris du secteur technologique. L'Organisation de coopération et de développement économiques (OCDE) a réaffirmé son intention de parvenir à une solution mondiale pour taxer l'économie numérique d'ici juillet 2021.

L'échange américain de crypto-monnaies Coinbase a rejoint le marché boursier.

Les banques centrales du Royaume-Uni et du Japon ont lancé des travaux exploratoires sur les monnaies numériques.

neutre

Infrastructure

Lors d'un sommet en ligne sur la résilience des semi-conducteurs et de la chaîne d'approvisionnement, le président américain Joe Biden a réitéré les plans visant à renforcer l'industrie des semi-conducteurs du pays et à sécuriser sa chaîne d'approvisionnement.

Les États-Unis ont ajouté sept entités chinoises de supercalculateurs à la liste de contrôle des exportations.

en progression

Droits numériques

Les données de 533 millions d'utilisateurs de Facebook ont été divulguées dans un forum de piratage en ligne. En outre, les données de 500 millions d'utilisateurs de LinkedIn ont été mises en vente. *Lire notre analyse aux pages 2, 6–7.*

TikTok a été poursuivi en justice au Royaume-Uni pour le traitement des données des enfants. Les organisations de consommateurs et de protection de l'enfance ont demandé à Facebook d'annuler ses projets de création d'un Instagram pour enfants.

en progression

Politiques des contenus

Facebook a élargi le champ d'action de son conseil de surveillance afin de statuer également dans les cas où l'entreprise a choisi de ne pas retirer un contenu. Le conseil a reporté sa décision sur l'interdiction de Facebook et d'Instagram pour Trump.

La plateforme de livestream Twitch a annoncé qu'elle allait bannir des utilisateurs en cas d'inconduite grave survenue en dehors de la plateforme.

Twitter a été critiqué pour avoir donné suite à une demande du gouvernement indien de supprimer les tweets considérés comme critiques à l'égard de la gestion de la pandémie de COVID-19 par le gouvernement.

Instagram a publié de nouvelles fonctionnalités pour lutter contre les discours haineux. Twitter a lancé une initiative visant à analyser l'impact néfaste de ses algorithmes.

en progression

Questions juridiques

La Cour suprême des États-Unis a rendu son avis dans l'affaire Google LL.C v. Oracle America InC., statuant que la copie d'une partie du programme informatique Java SE par Google est protégée en tant que « fair use ».

Une haute cour pakistanaise a levé l'interdiction de TikTok imposée par le régulateur des télécommunications du pays. Un tribunal russe a infligé une amende à Twitter pour ne pas avoir supprimé les contenus encourageant les mineurs à participer à des manifestations non autorisées.

Un tribunal d'Amsterdam a ordonné à Uber de réintégrer cinq chauffeurs exclus de la plateforme par un processus automatisé.

en progression

Nouvelles technologies (IdO, IA, etc.)

La Commission européenne a lancé un projet de règlement pour les systèmes d'IA. *Pour en savoir plus, voir page 10.* La Commission fédérale du commerce américaine a prévenu qu'elle prendrait des mesures contre les systèmes d'IA discriminatoires.

Le Brésil a adopté une stratégie en matière d'IA. Le Canada a présenté des plans pour la mise à jour de sa stratégie en matière d'IA et le lancement d'une stratégie quantique nationale. La Finlande a créé l'Institut quantique.

Le Royaume-Uni a présenté des plans visant à réglementer la cybersécurité des dispositifs de l'internet des objets.

« Scraping » de données et les problèmes auxquels sont confrontés les régulateurs et les utilisateurs

Le 3 avril, Business Insider a révélé qu'une base de données contenant les données personnelles de 553 millions d'utilisateurs de Facebook avait été téléchargée sur un forum de piratage. Quelques jours plus tard, une archive contenant les informations personnelles de 500 millions d'utilisateurs de LinkedIn a également été mise en vente.

Quelle est la différence entre le « scraping » de données, une violation de données et une fuite de données ?

Le **raclage *(scraping)* de données** est une extraction automatique de grandes quantités de données à partir de sites web, de bases de données ou d'applications. Dans ce cas, un programme « explore » le contenu d'un site web ou d'une plateforme et extrait ou copie automatiquement les informations accessibles au public, puis crée un document (feuille Excel, registre comptable, site web). Il s'agit d'une pratique courante dans les entreprises ; par exemple, c'est ce que font les moteurs de recherche pour nous fournir les informations que nous recherchons. C'est également la façon dont fonctionnent les sites web de comparaison de prix, comme ceux qui comparent les prix des billets d'avion ou les coûts des assurances.

Le *scraping* de données n'est pas illégal, mais il doit respecter certaines règles, telles que l'obligation d'obtenir le consentement des personnes concernées et une raison légale d'utiliser cette méthode. Les problèmes qui découlent de l'extraction de données sont liés à la manière dont les données sont extraites (avec ou sans consentement), à l'usage qui en est fait (analyse des données ou publication sur le site web de pirates) et à la responsabilité des risques et menaces.

On parle de **violation de données** lorsqu'un système informatique ou des données sont illégalement accessibles ou affaiblis par des acteurs malveillants à l'insu ou sans l'autorisation du propriétaire, ce qui entraîne l'exposition d'informations confidentielles, sensibles ou protégées. Les violations de données (ou hacks) sont illégales. Dans de nombreux cas, elles sont considérées comme un crime.

On parle de **fuite de données** lorsque des données privées (ou une base de données privée, même si elle est constituée de divers éléments de données accessibles au public) sont mises à la disposition du public. Une fuite de données ne nécessite pas une intrusion active dans un système informatique. Elle est généralement le résultat de mauvaises pratiques en matière de sécurité des données ou d'une erreur humaine accidentelle. La responsabilité des fuites de données est liée à l'obligation de préserver la sécurité des données et de prendre les mesures nécessaires à cet effet.

Les réponses immédiates de Facebook et de LinkedIn ont été similaires : les violations étaient des incidents de *scraping* à grande échelle, plutôt que des piratages. Cela a attiré l'attention des régulateurs de la protection des données et des utilisateurs du monde entier.

Facebook a déclaré que l'incident s'est produit en août 2019, lorsque des acteurs malveillants ont utilisé une vulnérabilité dans la fonctionnalité « Comment les gens peuvent me trouver », qui a ensuite été corrigée. Il est apparu par la suite que les données avaient été collectées à plusieurs reprises entre 2018 et 2019 (nous abordons la question de la chronologie plus bas). Dans le cas de LinkedIn, on ignore l'ancienneté de ces informations et si elles ont été agrégées uniquement à partir de la plateforme.

Voici au moins cinq grandes questions que les régulateurs doivent résoudre.

Problème n°1 : Comment les plateformes classent les données personnelles (privées ou publiques)

Les deux entreprises ont déclaré que les données étaient publiques. Dans le cas de Facebook, l'entreprise a ajouté qu'il incombe aux utilisateurs de s'assurer que « leurs paramètres correspondent à ce qu'ils souhaitent partager publiquement ». En d'autres termes, si un utilisateur choisit certains paramètres sur la plateforme, Facebook considère cela comme le consentement requis par certaines réglementations en matière de protection des données. Le problème ici est que Facebook n'explique pas correctement aux utilisateurs toute l'étendue des conséquences de certains paramètres pour que les utilisateurs puissent prendre une décision en connaissance de cause.

De plus, si l'on regarde la page de ressources dédiée, la plateforme indique que les informations publiques font référence à « certaines des informations que vous nous donnez lorsque vous remplissez votre profil… » ou que « votre profil public inclut votre nom, votre sexe, votre nom d'utilisateur… ». Le fait que Facebook parle en termes de « certaines » ou « incluant » laisse les utilisateurs dans l'ignorance. Par conséquent, les utilisateurs pourraient fournir des données personnelles à Facebook en pensant à tort que Facebook les gardera privées.

Problème n° 2 : La responsabilité des plateformes à l'égard des données personnelles qu'elles détiennent, qu'elles soient publiques ou non

Dans certaines juridictions, les plateformes sont effectivement responsables des données personnelles, même si elles sont déjà publiques et visibles par d'autres. Par exemple, le RGPD de l'UE stipule que les entreprises doivent mettre en place certaines mesures techniques pour garantir que les données personnelles sont traitées de manière sûre, sécurisée et conforme à la loi.

On peut donc affirmer que si les données ont été extraites des plateformes – que ce soit en raison d'une vulnérabilité du système ou de l'absence de détection des activités de *scraping* – les plateformes ont une part de responsabilité.

L'autorité irlandaise de protection des données, par exemple, va dans ce sens. Digital Rights Ireland, un groupe de défense des droits numériques, se prépare également à intenter un procès de masse contre Facebook au nom des utilisateurs qui veulent être dédommagés pour l'exposition de leurs données personnelles, en violation des conditions générales de la plateforme. Aux États-Unis, l'incident pourrait être considéré comme une violation de l'accord de 5 milliards de dollars conclu par Facebook avec la Commission fédérale du commerce (FTC) pour résoudre, entre autres, le scandale des données de Cambridge Analytica. D'autres procès d'utilisateurs devraient frapper Facebook en Inde et dans d'autres pays.

Problème n° 3 : La tentative des plateformes de normaliser des incidents récurrents

Facebook a minimisé l'incident non seulement pour se dégager de toute responsabilité, mais aussi pour le normaliser comme un événement chronique. Facebook dit aux utilisateurs et aux régulateurs que le monde doit s'habituer à de tels incidents et qu'il n'a pas l'intention d'informer les utilisateurs concernés à chaque fois que cela se produit.

Cette information provient d'e-mails internes qui ont circulé : « Nous nous attendons à d'autres incidents de *scraping* et nous pensons qu'il est important d'en faire un problème industriel général et de normaliser le fait que cette activité se produit régulièrement ».

Question n° 4 : L'obligation pour les plateformes de signaler une fuite de données

Les deux plateformes n'ont pas divulgué ni notifié ces incidents aux utilisateurs ou aux autorités à l'époque. Dans des pays comme les États membres de l'UE et le Brésil, qui disposent d'une réglementation complète en matière de protection des données, Facebook et LinkedIn s'exposent à de lourdes amendes en cas d'absence de divulgation et de notification des brèches et des violations de la réglementation en matière de protection des données.

En vertu du RGPD, et de manière similaire en vertu de son homologue brésilien, le LGPD, le *scraping* de données personnelles nécessite un consentement et une base légale. Le Commissaire irlandais à la protection des données et la Fondation brésilienne de protection et de défense des consommateurs de l'État de São Paulo – comme d'autres dans le monde – enquêtent sur les pratiques de Facebook. Des mesures similaires sont prises dans le cas de l'incident de LinkedIn, l'Agence italienne de protection des données ayant ouvert une enquête. La question cruciale pour les régulateurs est d'établir, en termes juridiques, comment ces violations relèvent du type d'incidents qui déclencherait la responsabilité des plateformes de les signaler.

C'est ici qu'intervient la chronologie : La date à laquelle la violation (ou la fuite) a eu lieu a un impact direct sur la responsabilité des plateformes. En Europe, par exemple, signaler une violation est devenu une obligation légale lorsque le RGPD est entré en vigueur en mai 2018.

Aux États-Unis, Facebook est dans une certaine mesure protégé de toute responsabilité pour les violations survenues avant juin 2019, dans le cadre de l'accord Facebook/Cambridge Analytica, sauf dans l'État de Californie, où la loi sur la confidentialité des consommateurs est entrée en vigueur mi-2018. Pourtant, les régulateurs devront encore évaluer les ensembles de données composées et identifier le moment où les données qu'ils incluent, pour ensuite déterminer quand les plateformes ont appris les incidents de *scraping*, et quelles étaient les responsabilités de Facebook et LinkedIn à ce moment-là.

Question n° 5 : Les utilisateurs doivent être davantage sensibilisés aux risques liés à l'exposition des données personnelles et être protégés contre ces risques

Les données personnelles dans le domaine public peuvent être utilisées pour nuire à des personnes. Que la responsabilité en incombe aux utilisateurs (qui partagent des données personnelles sur les médias sociaux sans en comprendre les implications) ou aux plateformes (qui ne font pas assez pour protéger les données), des acteurs malveillants les exploiteront.

Dans ces deux cas, par exemple, la valeur des fuites réside dans la possibilité d'associer des numéros de téléphone mobile et d'autres données personnelles à un individu. Les fraudeurs qui appellent une personne sur un téléphone portable auront l'air plus authentiques et légitimes s'ils connaissent également sa date de naissance, sa ville natale et son lieu de travail. On pourrait penser que seules les autorités et leur banque détiennent de telles informations, non ?

Les entreprises elles-mêmes, victimes d'acteurs malveillants qui ont exploité les vulnérabilités de leurs platesformes, devront engager des poursuites judiciaires, comme elles l'ont déjà fait par le passé, mais cela devrait également servir d'avertissement aux utilisateurs. Comme l'a dit un organisme de protection des consommateurs : « Les gens seront beaucoup plus sceptiques et beaucoup plus prudents avant de fournir toute cette masse d'informations aux plateformes de réseaux sociaux ».

Le monde a besoin de plus de puces électroniques : Ce que cela signifie pour les grands acteurs

Une pénurie mondiale : comment en est-on arrivé là ?

Les semi-conducteurs – ou puces électroniques – sont au cœur de pratiquement tous les appareils électroniques. La production de ces puces repose sur une chaîne d'approvisionnement mondiale très complexe. La production d'une seule puce informatique peut impliquer plus de 1 000 étapes et 70 passages de frontières distincts.

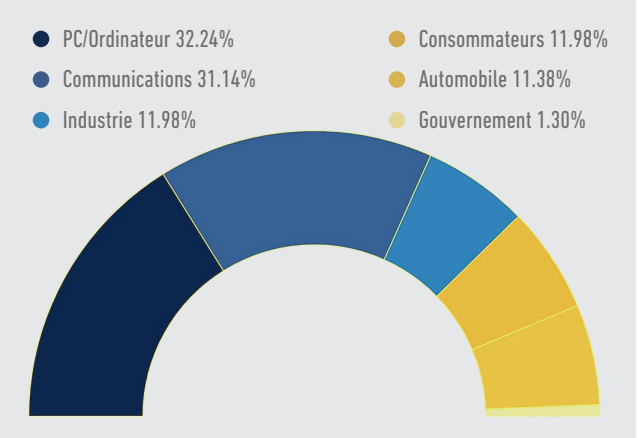
Elle implique l'extraction et le traitement des matières premières (telles que le silicium et le bore), la conception de la puce et le développement de l'équipement de fabrication. Tout cela doit se faire avant que la minuscule puce ne soit réellement fabriquée et assemblée.

Les États-Unis dominent les composantes d'architecture et de conception de la chaîne d'approvisionnement. Les entreprises américaines, Intel en tête, représentent près de 50 % des ventes de puces dans le monde. Mais plus de 80 % de la fabrication mondiale de puces se fait en Asie, avec Taiwan Semiconductor Manufacturing Company (TSMC) et Samsung en tête.

Actuellement, il y a une pénurie mondiale de puces, qui affecte les entreprises et, indirectement, les consommateurs. Samsung, lui-même fabricant de puces, a mis en garde contre un « grave déséquilibre entre l'offre et la demande de puces dans le secteur informatique à l'échelle mondiale ».

Apple aurait dû reporter la production de certains ordinateurs portables et tablettes en raison de la pénurie de puces et de composants d'affichage. Sony a rencontré des difficultés pour fournir sa nouvelle PlayStation 5. La pénurie devrait durer jusqu'en 2022 ou 2023.

L'une des raisons est que les fabricants de puces – et il s'agit essentiellement de TSMC, Samsung et, dans une moindre mesure, Intel – sont sensibles aux pics de la demande. La pandémie a généré une demande plus forte que d'habitude pour les smartphones, les ordinateurs portables et autres

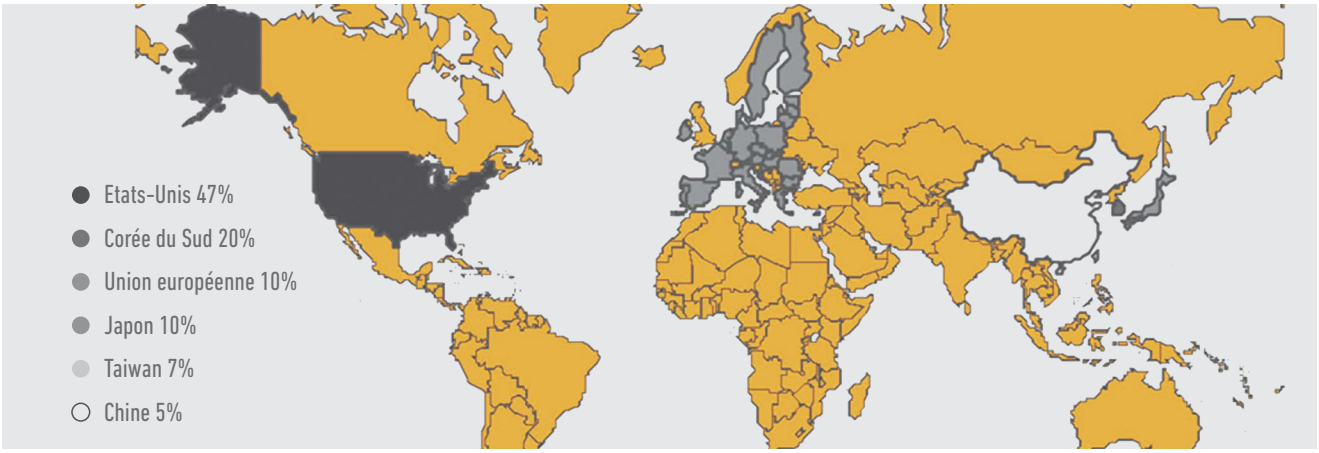


Consommation mondiale des puces électroniques. Source: Semiconductor Industry Association

appareils similaires, ce qui a incité les producteurs à augmenter leur demande. La demande provient également d'autres industries, comme les constructeurs automobiles et les producteurs d'appareils de l'internet des objets.

La poignée d'entreprises qui produisent des puces a eu du mal à répondre à cette demande. Les appareils numériques deviennent de plus en plus sophistiqués, tout comme la conception des puces. Cette évolution a entraîné une augmentation des coûts pour les fabricants de puces, ce qui constitue un obstacle pour les nouveaux acteurs désireux d'entrer sur le marché. Il en résulte un marché très concentré dans lequel seule une poignée d'entreprises peut se permettre de rivaliser et de répondre à la demande mondiale.

Les tensions géopolitiques, notamment les politiques de contrôle des exportations et d'octroi de licences imposées par le gouvernement américain aux entreprises chinoises ces dernières années, n'ont pas aidé. Par exemple, il est désormais interdit aux entreprises américaines et étrangères d'utiliser la propriété intellectuelle et la technologie américaines pour produire des puces pour Huawei (y compris les puces Kirin conçues par Huawei).



Parts de marché en 2020. Source: Semiconductor Industry Association

Avant l'entrée en vigueur de ces sanctions, Huawei a été contraint de stocker des puces, et des rapports affirment que de grands producteurs tels que TSMC ont donné la priorité aux commandes de Huawei au détriment d'autres clients, ce qui a affecté la chaîne d'approvisionnement avec des effets à long terme. Le fabricant de puces chinois Semiconductor Manufacturing International Corporation (SMIC) ne peut acquérir des technologies américaines que si ses fournisseurs reçoivent une licence du gouvernement américain.

Les catastrophes et incidents naturels affectent également la production et l'approvisionnement en puces. Des usines de puces ont dû fermer ou réduire leur production. Parmi elles, des usines au Texas (fermées en février 2021 en raison de pannes de courant causées par des températures basses) ; au Japon (après un incendie survenu en mars 2021) ; et à Taïwan (en raison de la sécheresse en cours).

Géopolitique : Comment les principaux acteurs mondiaux ont réagi

La Chine et les États-Unis, qui sont depuis longtemps en concurrence dans le secteur technologique, ont de grandes ambitions. Ils veulent tous deux devenir autonomes sur le marché des puces électroniques. Cela permettrait à leurs industries technologiques nationales de ne pas dépendre de mécanismes d'approvisionnement mondiaux externes, éventuellement instables.

On estime qu'un pays a besoin d'un minimum de 1 000 milliards de dollars au départ pour parvenir à une chaîne d'approvisionnement locale autosuffisante ; un tel investissement, à son tour, entraînerait une augmentation de 35 à 65 % du prix des puces. C'est énorme.

Ces dernières années, la Chine a été un importateur net de puces. Seulement 30% de ses puces ont été fabriquées dans le pays. Les sanctions commerciales et les contrôles à l'exportation imposés par les États-Unis et leurs effets sur des entreprises chinoises comme Huawei et SMIC ont alimenté les ambitions de la Chine de devenir autonome.

En conséquence, la Chine investit massivement dans ses propres capacités de fabrication de puces, dans le cadre de son plan quinquennal de plusieurs milliards de dollars. Publié en mars 2021, ce plan prévoit un soutien considérable à l'industrie locale des semi-conducteurs.

Les États-Unis ne produisent pas non plus suffisamment de puces par eux-mêmes, ce qui rend leur importante industrie technologique fortement dépendante des fabricants asiatiques. Lors d'un sommet organisé en avril, le président Joe Biden s'est engagé à renforcer l'industrie des semi-conducteurs du pays.

Biden a également demandé au Congrès de créer un fonds de 50 milliards de dollars pour la fabrication et la recherche dans le domaine des semi-conducteurs, conformément au projet de loi *CHIPS for America* actuellement débattu au Congrès (H.R. 7178/S. 3933).

On s'attend à ce qu'une partie de ce fonds serve à soutenir le développement d'usines de puces avancées aux États-Unis par TSMC, Samsung et Intel.

Si l'autosuffisance totale en matière de puces est une tâche presque impossible, le mieux est encore de s'approvisionner en puces ailleurs. Tant la Chine que les États-Unis s'appuient désormais sur la société taïwanaise TSMC, qui a réussi jusqu'à présent à naviguer dans les complexités géopolitiques entre les deux pays en se rendant indispensable aux deux.

Il n'est pas surprenant que TSMC soit maintenant confronté à une pression accrue pour choisir entre l'accès au plus grand marché de puces du monde aux États-Unis et celui de la Chine, qui connaît la croissance la plus rapide.

La pénurie de puces et la complexité de la chaîne d'approvisionnement offrent également une opportunité pour de nouveaux partenariats technologiques. L'UE, par exemple, a des options intéressantes devant elle, alors qu'elle tente d'atteindre son objectif de produire un cinquième des puces avancées au niveau mondial d'ici à 2030.

D'une part, elle pourrait unir ses forces à celles des États-Unis pour contrebalancer la concentration régionale de la production de puces en Asie. De l'autre, elle pourrait également s'associer à TSMC et/ou Samsung pour construire ou développer des usines en Europe. Bien entendu, le bloc pourrait également choisir d'investir davantage dans les acteurs européens.

Un autre partenariat potentiel se situe entre les États-Unis, le Japon, la Corée et l'Inde (connus sous le nom de « Quad »), qui ont récemment convenu de créer un groupe de travail sur les technologies critiques et émergentes. L'un des objectifs du Quad est de coopérer à la diversification des chaînes d'approvisionnement en technologies critiques.

L'adage « si vous ne pouvez pas les battre, rejoignez-les » ne pourrait être plus vrai.

Les règles proposées par l'UE pour réglementer les systèmes d'IA : Le bon, la brute et le truand

L'IA est partout autour de nous, de nos moteurs de recherche aux appareils intelligents que nous utilisons dans nos foyers. L'industrie continue de repousser les limites de ce que les systèmes d'IA peuvent faire. Des systèmes nouveaux et améliorés rendent nos vies plus confortables, nos décisions plus faciles à prendre et notre environnement plus sûr.

Tout cela semble bienheureux… jusqu'à ce que cela ne le soit plus. L'UE estime que des limites doivent être fixées en fonction du niveau de risque pour les personnes ou infrastructures. Au-delà de ces limites, les systèmes d'IA devraient être purement et simplement interdits (ou fortement réglementés). Voici l'approche fondée sur les risques qu'adopte la nouvelle proposition de la Commission européenne :

- **Les systèmes qui présentent un risque énorme seront considérés comme carrément inacceptables.** Les cas sont énumérés spécifiquement dans le règlement, et comprennent des types de reconnaissance faciale, et des algorithmes utilisés pour manipuler la façon dont nous pensons ou ce que nous faisons.
- **Les systèmes qui présentent un risque élevé feront l'objet d'un examen approfondi.** Il s'agit notamment des infrastructures critiques qui pourraient s'avérer risquées pour la vie des gens, et de certains composants de sécurité dans les produits (pensez à la chirurgie assistée par robot). Le règlement comprend à la fois une liste prédéfinie de cas et un ensemble de critères permettant de déterminer comment d'autres systèmes pourraient être classés comme à haut risque. Si un système est jugé à haut risque, il doit être évalué avant d'être mis sur le marché, puis enregistré. Il y a en fait une foule d'autres obligations impliquées, et bien sûr, des sanctions en cas de non-respect de celles-ci.
- **Les systèmes qui présentent un risque limité ne comporteront que des obligations mineures.** Parmi ceux-ci figurent les *chatbots* : Les règles exigeront que l'on soit au moins informé que l'on parle avec une machine.
- **Les systèmes qui présentent un risque minimal peuvent être développés et utilisés librement.** Essentiellement, il s'agit de tout ce qui ne relève pas des trois ci-dessus. La plupart des systèmes d'IA actuellement utilisés entrent dans cette catégorie.

La prochaine étape est l'examen de la proposition par le Parlement européen et les États membres. Cela semble simple, mais il faudra en réalité des années de lectures, d'amendements et de lobbying avant que la réglementation ne soit adoptée.

La proposition suscite des réactions mitigées

Les règles proposées ont été critiquées pour leur langage vague et général, et pour ne pas aller assez loin. Elles sont également truffées de lacunes, notamment en ce qui concerne les technologies de reconnaissance faciale et leurs pratiques souvent discriminatoires.

Par exemple, les systèmes qui identifient les personnes par des données biométriques en temps réel sont généralement interdits. Cependant, il existe certaines exceptions qui s'appliquent aux forces de l'ordre et qui, selon les critiques, peuvent donner lieu à des abus.

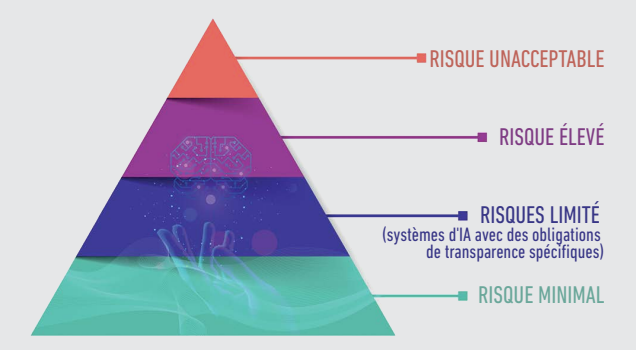
De plus, l'interdiction ne s'applique pas aux autres entités publiques ou aux entreprises. Qui sait si elles utilisent déjà la biométrie en temps réel ? Les activistes affirment qu'elles le font, en fait.

La biométrie en temps réel est peut-être interdite, mais les systèmes qui fonctionnent sur des images pré-captées ne le sont pas. Ces systèmes peuvent toujours être utilisés pour identifier des personnes en fonction de leur race, de leur sexe et de leur sexualité. Par conséquent, même s'ils sont fortement réglementés, les entreprises pourraient obtenir le feu vert pour les utiliser.

Et puis, il y a la question de l'équilibre entre innovation et réglementation. Les entreprises pensent qu'il y a trop d'obligations de conformité en place. Cet argument ne suffira pas à Margrethe Vestager, vice-présidente exécutive de la Commission européenne, qui est catégorique : l'Europe « ne pourra tirer pleinement parti du potentiel sociétal et économique de l'IA que si nous sommes convaincus de pouvoir atténuer les risques associés ».

Toutefois, la situation se complique lorsque les entreprises affirment que la loi va ralentir le développement de systèmes d'IA avancés dans l'UE. Bien que les grandes entreprises puissent trouver cela difficile – mais pas impossible – les petites entreprises ou les start-ups pourraient être complètement découragées.

La Commission souhaite certainement que l'Europe fasse confiance au développement des systèmes d'IA, mais elle veut également encourager une industrie locale. Comme nous l'avons dit dans notre commentaire (page 2), l'UE va marcher sur une corde raide et aura des décisions difficiles à prendre.



Récents développements au sein 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 en avril. Pour d'autres comptes rendus d'événements, consultez la section Past Events sur l'observatoire *GIP Digital Watch*.

Protection des infrastructures critiques liées à l'eau (partie II) 13 avril 2021

Cet événement, organisé par les missions permanentes de la Slovénie et d'Israël à Genève, l'Organisation météorologique mondiale (OMM) et Microsoft, faisait suite à la table ronde de novembre 2020. Cette deuxième partie a permis d'étudier comment certains des enseignements tirés de la table ronde pourraient être appliqués dans les pays en développement, notamment dans la région africaine. L'événement s'est concentré sur les expériences nationales, ainsi que sur les cadres et les normes qui ont été mis en place, tels que la Convention de Malabo.

Promouvoir l'économie circulaire et l'utilisation durable des ressources naturelles dans la région de la CEE-ONU 20–21 avril 2021

La Commission économique des Nations Unies pour l'Europe (CEE-ONU) a axé sa 69e session sur l'économie circulaire et l'utilisation des ressources naturelles pour atteindre les ODD. L'une des tables rondes portait sur l'énergie circulaire, la mobilité et la transformation numérique, ainsi que sur les nouvelles politiques et les meilleures pratiques industrielles. Alors que l'énergie aspire à être à faible teneur en carbone ou à carbone négatif, il y a également une forte poussée pour l'e-mobilité (véhicules à moteur électrique) dans les villes et pour le transport sur de longues distances. La technologie est au cœur de la quatrième révolution industrielle, qui touche tous les aspects de la vie et du travail. La transformation numérique a une incidence importante sur la façon dont les ressources naturelles sont utilisées, en abandonnant les modèles linéaires du passé au profit de nouveaux modèles commerciaux durables, axés sur les services et l'économie circulaire.

Économie numérique : Tournée du commerce et des finance 28 avril 2021

Cette table ronde, organisée par le GIP dans le cadre de la série 12 tournées pour naviguer dans la Genève numérique, a débattu des discussions en cours sur le commerce électronique au sein de l'Organisation mondiale du commerce (OMC), une attention particulière ayant été accordée à l'Initiative de la déclaration conjointe et aux accords commerciaux régionaux. Les intervenants se sont également penchés sur les impacts de la pandémie de COVID-19 sur le commerce électronique et sur le rôle que ce dernier peut jouer dans le monde post-pandémique.

Ce qu'il faut surveiller : Les événements relatifs aux politiques numériques du mois de mai

Jetons un coup d'œil au calendrier mondial de la politique numérique. Voici ceux qui auront lieu le mois prochain dans le monde entier, avec des liens directs vers les sites web et les programmes officiels des événements. Pour encore plus d'événements, visitez la section Événements de l'observatoire *Digital Watch*.

May

5–7 mai, Forum 2021 sur la science, la technologie et l'innovation (STI) (en ligne)

Le 6e Forum STI se tiendra sous le thème « Science, technologie et innovation pour une reprise durable et résiliente du COVID-19, et voies efficaces d'action inclusive vers les objectifs de développement durable ». Le forum traitera de la coopération en matière de STI, de la manière de mettre les technologies au service des ODD et des répercussions de l'évolution technologique rapide sur les ODD à la lumière de la pandémie de COVID-19. *Nous publierons les rapports de certaines sessions.*

17–21 mai, Semaine finale du Forum 2021 du SMSI (en ligne)

Le Forum 2021 du SMSI, qui se déroule depuis janvier, s'achèvera par une dernière semaine consacrée à des dialogues interactifs de haut niveau, à des cérémonies de remise de prix et de récompenses, à une table ronde ministérielle et à des réunions de facilitation de la ligne d'action du SMSI. *Comme d'habitude, nous publierons les rapports de session de cette dernière semaine.*

25–28 mai, 13e Conférence internationale sur les cyberconflits (CyCon 2021) (Tallinn, Estonie)

Accueillie par le Centre d'excellence OTAN en matière de cyberdéfense coopérative, la conférence CyCon 2021 a pour thème central « Devenir viral ». Les participants discuteront des implications des crises humaines – telles que la pandémie COVID-19 – pour la cybersécurité et le cyberespace.

17–20 mai, RSA Conference 2021 (en ligne)

Sous le thème « Résilience », RSA 2021 accueillera des sessions pratiques éducatives, ainsi que des sessions traditionnelles dirigées par des conférenciers et des discours d'ouverture. Les sujets à l'ordre du jour de cette année comprennent le renseignement, la gouvernance politique, la lutte contre la fraude, les pirates et les menaces, l'identité, l'apprentissage automatique et l'IA, les outils open source et la vie privée.

24–29 mai, Session finale du sixième Groupe d'experts gouvernementaux de l'ONU (en ligne)

Le sixième Groupe d'experts gouvernementaux des Nations Unies est sur le point de conclure ses travaux. Le groupe a été mandaté pour étudier les menaces existantes et potentielles dans le domaine de la sécurité de l'information, ainsi que les mesures de coopération possibles pour y faire face. Il a également été chargé d'étudier comment le droit international s'applique à l'utilisation des TIC par les États, ainsi que d'examiner les normes, règles et principes de comportement responsable des États et les mesures de confiance nécessaires. *Nous publierons des mises à jour sur notre espace dédié.*

31 mai–11 juin, École sur la gouvernance de l'Internet, les politiques numériques et l'innovation (SIDI) (en ligne)

La deuxième édition de la SIDI s'adresse aux étudiants diplômés et aux professionnels – principalement de l'Europe du Sud-Est et de la région voisine (SEE+) – désireux d'en savoir plus sur l'innovation numérique, l'impact de l'internet et des autres technologies numériques sur la société et l'économie, et les multiples dimensions de la politique numérique et de la gouvernance de l'internet. Diplo, l'opérateur du GIP, est un partenaire officiel de la SIDI.

June

A propos de ce numéro

Numéro 59 de la newsletter *Digital Watch*, publié le 30 avril 2021 par la Geneva Internet Platform et DiploFoundation | Contributeurs: Katarina Anđjelković, Stephanie Borg Psaila (editor), Andrijana Gavrilović, Tereza Horejsova, Pavlina Ittelson, Marco Lotti, Virginia (Ginger) Paque, Nataša Perućica, et Sorina Teleanu | Traducteur de l'édition française: Clément Perarnaud | Design: Aleksandar Nedeljkov, Viktor Mijatović, et Mina Mudrić, Diplo's CreativeLab | Contactez-nous: digitalwatch@diplomacy.edu

Couverture

En l'IA nous croyons ? 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