Géopolitique des données (Data geopolitics)

Petit livre de lectures
(Little reading book)

[Assembled and formatted for e-book readers by Wergosum on 20200411 … and later expanded]

Table des matières/Contents

1. La géopolitique de la bataille des données

20171217

Stéphane Bussard

Le centre de données d'Advania Thor, à Hafnarfjördur, dans l'ouest de l'Islande. — © Sigtryggur Ari / Reuters

Source: https://www.letemps.ch/monde/geopolitique-bataille-donnees

Alors que s’ouvre ce lundi à Genève le 12e Internet Governance Forum, la guerre autour du contrôle du data fait rage. Si la Chine et la Russie estiment que la régulation du web relève de la responsabilité des gouvernements, les membres de l’OCDE et la Silicon Valley estiment que les sociétés technologiques et la société civile doivent faire partie du processus d’encadrement du cyberespace

Façonner le futur numérique.

A l’heure où s’ouvre ce lundi la 12e édition de l’Internet Governance Forum au Palais des Nations à Genève, le

cyberespace est le théâtre d’une féroce bataille géopolitique: celle des données. «Le data, c’est le pétrole de la nouvelle économie», relève Jovan Kurbalija. Pour le directeur de la DiploFoundation et responsable de la Geneva Internet Platform, «le statut qu’on attribuera aux données déterminera le futur de nos sociétés.»

Les deux côtés de l’échiquier

A une extrémité de l’échiquier, il y a les GAFA, les grandes sociétés d’Internet que sont Google, Amazon ou Facebook. Pour elles, «c’est un peu la conquête du Far West, une captation sans fin des données», déplore Solange Ghernaouti, professeure à l’Université de Lausanne

et directrice du Swiss Cybersecurity Advisory and Research Group. Si ces géants de la Silicon Valley sont désormais dans le collimateur du politique pour avoir poussé leurs prérogatives trop loin, nombre de pays de l'OCDE estiment que le processus visant à encadrer Internet ne pourra se faire sans elles. C'est sans doute la raison pour laquelle le président de Microsoft, Brad Smith, a pris les devants en appelant à la création d'une Convention de Genève numérique dans laquelle son entreprise aurait son mot à dire.

De l'autre côté de l'échiquier, il y a les pays dont les gouvernements

considèrent qu'il est de leur seule responsabilité de cadrer Internet, notamment à travers un traité international classique. C'est le cas du Groupe des 77, une coalition de pays en développement ainsi que de la Chine et de la Russie. La Chine, dont la société civile est faible, insiste sur sa souveraineté quand il est question du cyberespace.

Un véritable séisme

Dans cette bataille géopolitique, l'Union européenne pourrait être le grand trublion. Bruxelles vient d'édicter un règlement général sur la protection des données (RGPD), qui entrera en vigueur le 25 mai 2018. «Un véritable

séisme, explique le directeur de la DiploFoundation. Les sociétés internet devront demander l'accord des citoyens pour utiliser les données les concernant. Les implications sont considérables. Car en cas de non-respect, les amendes seront très salées: 4% du chiffre d'affaires.» Le RGPD n'est pas pris à la légère par les géants de la Silicon Valley, qui sont déjà en train de louer d'énormes espaces de bureaux dans la capitale européenne.

Une guerre de titans

Dans cette guerre de titans, deux acteurs vont se profiler au cours des cinq prochaines années: Bruxelles, au vu de sa puissance politique et économique, et

Genève, pour son soft power. Selon Jovan Kurbalija, la ville du bout du Léman n’est pas une économie de niche comme la Silicon Valley. C’est un écosystème qui permet de traiter des datas sous tous leurs aspects, que ce soit à l’OMC pour les questions économiques, au CICR pour la protection de données ultrasensibles – qui peut être une question de vie ou de mort dans certains conflits –, au Conseil des droits de l’homme pour la protection de la sphère privée ou à l’Union internationale des télécommunications pour les infrastructures techniques. «De telles organisations internationales devront toutefois aussi se conformer à la

RGPD», précise le directeur de la DiploFoundation. Conseiller d'Etat genevois, Pierre Maudet abonde dans le même sens. Genève a un rôle à jouer grâce aux soft laws, aux normes qui permettront d'instaurer une confiance numérique.

La position de la Suisse

Entre les deux extrêmes, des pays comme l'Inde, la Suisse et le Brésil essaient de trouver un espace pour un accord éventuel. Avec sa stratégie «Suisse numérique», la Confédération s'adapte. Vice-directeur de l'Office fédéral de la communication, Thomas Schneider le relève: «Nous cherchons à trouver une nouvelle politique de

données qui permette au secteur privé de développer des applications et des services innovants et respecte en même temps le droit individuel de maintenir un contrôle sur ses propres données. Nous voulons rester compétitifs sans lâcher du lest sur les droits fondamentaux propres à une démocratie.» Il nuance toutefois: «Il ne suffit pas de collecter des données, il faut aussi savoir qu'en faire.»

Une chance de progrès social

La professeure Solange Ghernaouti le reconnaît: la Chine a compris la nécessité de garder sa souveraineté sur ses données. Les sinologues les plus critiques craignent toutefois que

l’accumulation considérable de données sur les citoyens ne renforce le pouvoir autoritaire de Pékin. Pour Solange Ghernaouti, le débat actuel sur les données devrait être une chance de transformer le progrès économique en progrès social, mais elle met en garde: «Le politique ne doit pas être à la solde de l’économie.»

2. La Chine exacerbe la bataille pour le contrôle d’internet

Stéphane Bussard

20200407

Source: https://www.letemps.ch/monde/chine-exacerbe-bataille-controle-dinternet

Une délégation d'ingénieurs chinois, notamment de Huawei, ont proposé à l'UIT à Genève une nouvelle infra-structure d'internet pour remplacer celle dominée par les sociétés techno-logiques américaines. Certains y voient le début d'une guerre sanglante pour le contrôle de la Toile, d'autres relativisent. Etat des lieux

Vue du bâtiment de l'Union internationale des té-lécommunications (à gauche) et de l'Organisa-tion mondiale de la propriété intellectuelle à Geneve. — © KEYSTONE/Martial Trezzini

En février, ils étaient près de 180 personnes réunies dans une salle de l’Union internationale des télécommunications (UIT) établie à deux pas de la place des Nations à Genève. Motif: écouter une équipe d’ingénieurs chinois présenter un nouvel IP (protocole internet) au nom de Huawei, de China Unicom, de China Telecom et du Ministère chinois de l’industrie et de la technologie de l’information. Une infrastructure totalement nouvelle d’internet. Par le passé, diverses alternatives à l’internet actuel, dominé par les sociétés technologiques américaines, les Gafam, ont déjà été présentées. Mais cet épisode, raconté récemment par le

Financial Times (FT), apparaît comme la bataille la plus sérieuse jamais menée pour contrôler la Toile. Un combat qui se superpose à la rivalité géopolitique entre les Etats-Unis et la Chine, d'une part, et au modèle de société démocratique ou autoritaire, de l'autre.

Autorité étatique

A l'UIT, agence des Nations unies responsable de nombreux standards dans ce domaine, le nouvel IP chinois, apparemment en phase d'élaboration, a été expliqué au moyen d'un Powerpoint, mais sans grands détails. La démonstration a cependant eu pour but de montrer que l'internet actuel n'est plus à la hauteur des nouvelles

technologies, de la communication par hologrammes, des voitures autonomes ou de la chirurgie à distance. A en croire le FT, la Russie soutiendrait la proposition chinoise. Des Etats comme l'Iran, l'Arabie saoudite seraient aussi intéressés par un modèle prônant une gestion «top down» d'internet où l'Etat jouit d'une pleine souveraineté d'internet.

Que faut-il dès lors penser du nouvel IP chinois? L'un des pères de l'internet suédois et conseiller digital du gouvernement à Stockholm, Patrik Fältström, est très critique. «Une chose m'irrite. La proposition chinoise dit résoudre tous les problèmes d'internet,

mais on ne sait pas lesquels.» Il craint que le nouvel IP chinois confère à l'Etat l'autorité absolue de dire qui pourrait se connecter à internet. A voir la manière dont Pékin gère internet, cette perspective fait figure d'épouvantail. Il le relève: «Même si on est captif des big techs, on peut toujours choisir de ne pas utiliser Google.»

Directeur de la DiploFoundation à Genève et responsable de la Geneva Internet Platform, Jovan Kurbalija estime que la proposition chinoise a plusieurs mérites: «Elle a été bien testée dans les milieux académiques. Elle est discutée dans un processus régulier de l'UIT et peut être mise en œuvre

rapidement par Huawei et de grandes sociétés chinoises.» Jovan Kurbalija poursuit: «De nombreuses organisations ont déjà travaillé sur un nouveau protocole internet, que ce soit l’Internet Engineering Task Force, Google avec son Quick ou Mozilla par son DNS via HTTP. La proposition chinoise n’est qu’une compilation de ces efforts, de projets académiques.»

Le directeur de la DiploFoundation ajoute: «Pour la première fois, la Chine montre une supériorité intellectuelle à l’échelle globale. Elle n’agit pas comme seule fabricante de produits, mais donne une nouvelle direction au domaine de la technologie.» Contacté, l’Office fédéral

de la communication (Ofcom) est prudent: «Il est encore trop tôt pour donner une évaluation sérieuse. Les discussions sur le thème de nouvel IP en sont à leurs débuts au sein de l'UIT, où le terme n'a pas encore été clairement défini.»

Problèmes surtout politiques

La liberté d'internet et la démocratie sont-elles menacées par le projet chinois, comme le laisse entendre le FT? Chercheur à l'Université d'Amsterdam, Niels ten Oever réfute cette analyse: «On ne résout pas des problèmes politiques voire économiques avec la technologie.» Si on veut un internet plus horizontal, il faudrait déjà

que des Etats et universités qui confient leur messagerie à Google y renoncent et gèrent leurs propres réseaux. «Il faut éviter d'aller vers une gouvernance algorithmique.» Le chercheur ajoute: «Le nouvel IP chinois, c'est du vieux vin dans une nouvelle bouteille. Pour l'heure, ce n'est qu'une proposition. Or je vous rappelle qu'à l'heure actuelle, 9000 standards internet ne sont pas appliqués. Internet est un cimetière d'idées. Pour moi, la question n'est pas de savoir si l'on veut un internet géré par des multinationales qui s'autorégulent ou si on veut qu'il le soit par l'Etat. Nous Européens, avec notre fibre sociale-démocrate, nous souhaitons les deux!»

Niels ten Oever nous rafraîchit la mémoire: «Je rappelle qu'au départ, internet était un projet public. Les Etats ont pris tous les risques et ce n'est qu'après que des sociétés commerciales s'y sont intéressées et ont engrangé tous les bénéfices. Jusqu'en 1993, aucun projet commercial n'était autorisé sur la Toile. C'est donc à nous de savoir ce que nous voulons. La bataille des standards n'est en tout cas pas nouvelle. Elle existe depuis longtemps dans des organismes comme l'ICANN et l'UIT. Ce qu'il importe de savoir maintenant, c'est comment construire une infrastructure publique sur un réseau privé.»

Jovan Kurbalija ne voit pas la Chine avancer seule. Pékin n’a pas besoin d’un nouveau protocole internet pour contrôler son internet. Il le contrôle déjà totalement. Mais la Chine, superpuissance technologique, a les moyens d’influencer d’autres pays. «La Chine ne peut pas faire cavalier seul, car si elle refuse de trouver un compromis avec l’Union européenne, elle risque de perdre l’accès au grand marché européen ainsi qu’à d’autres marchés de pays en voie de développement. Je pense qu’elle sera disposée à trouver un compromis.» L’Ofcom tempère: «L’état actuel des discussions, qui se trouvent à leur tout début, ne permet pas d’évaluer

si un consensus sur le nouvel IP sera trouvé au sein de l’UIT.»

Fragmentation

Le Financial Times met en garde contre l’émergence d’un «patchwork d’internets nationaux». Niels ten Oever n’y croit pas: «Internet est toujours interconnecté. C’est en réalité le consommateur qui le fragmente en décidant de ne pas en explorer certaines parties.» Directrice du Swiss Cybersecurity Advisory and Research Group de l’Université de Lausanne, Solange Ghernaouti relativise: «Cela fait quinze ans que l’on parle d’une balkanisation d’internet, d’une réappropriation nationale de la Toile.»

Depuis le Sommet mondial de la société de l’information en 2003 à Genève, on s’interroge sur la manière de sortir du pur contrôle américain. Cela a donné naissance à l’Internet Governance Forum en 2006.

Depuis, ajoute Solange Ghernaouti, des progrès ont été constatés pour ce qui concerne la gestion des adresses IP et des noms de domaines, dont dépend l’accès à internet. L’alphabet alphanumérique n’est plus le seul autorisé. L’initiative chinoise va au-delà en proposant d’autres manières de contrôler l’accessibilité au réseau. Plus récemment, sous l’égide de l’Unesco, il y a eu l’appel de Paris d’Emmanuel

Macron: «Pour la confiance et la sécurité dans le cyberespace».

Solange Ghernaouti le constate: «Nous sommes dans une guerre géopolitique pour la maîtrise de l’infrastructure et des données personnelles et industrielles. Pékin veut prendre le contrôle de l’appareil de production numérique mondial, c’est le sens de la bataille autour de la 5G et d’un nouvel internet. Peut-être va-t-on redécouvrir l’importance du multilatéralisme et celle prise par notre dépendance numérique.»

Ambassadrice des Pays-Bas pour l’économie digitale, Lousewies van der Laan nuance dans un courrier des

lecteurs adressé au FT. Pour elle, internet n’est pas cassé. Malgré des sous-investissements dans les centres de données et la fibre, l’infrastructure technique d’internet tient bien la route. S’il y a des problèmes, poursuit-elle, ils sont avant tout politiques. En fin de compte, la solution à terme «n’est pas davantage de contrôle étatique sur internet, comme la Chine et la Russie l’ont proposé à l’UIT». Pour la diplomate, les Etats doivent plutôt s’assurer que les cybercriminels soient poursuivis, que les big techs paient des impôts, que les données soient protégées, que les normes de sécurité soient appliquées et enfin que la population soit mieux formée.

Dans la bataille pour le contrôle d’internet, quel rôle pour l’Union internationale des télécommunications? A l’UIT, cela fait des années que l’on parle de la future gouvernance d’internet. Et puis en février 2017, il y eut l’appel de Brad Smith, le président de Microsoft, pour une Convention de Genève numérique. Aujourd’hui, il y a l’initiative chinoise de nouvel IP. Chef du Département des commissions d’étude dans le secteur de la normalisation de l’UIT, Bilel Jamoussi en est convaincu: «L’UIT continue de jouer le rôle de hub pour le dialogue technologique. Elle reste d’autant plus importante que les normes utilisées pour

internet relèvent en très grande partie de ses compétences.» Pour lui, il faut passer à la vitesse supérieure, avoir une bande passante beaucoup plus large, une connectivité et une sécurité renforcées. Le nouvel IP chinois n’est pas une tentative de rajouter une couche au réseau existant. «C’est un changement de paradigme. Mais un consensus n’est pas pour demain.»

Les discussions vont se poursuivre au sein du Comité technique 13 de l’UIT présidé par le Suisse Leo Lehmann. La proposition chinoise sera à nouveau débattue en Inde en novembre. Les pressions sur l’UIT sont énormes. Certains déplorent que la prolifération

des forums se penchant sur internet à Genève crée une grande confusion. Ils se demandent si le débat sur la future gouvernance d'internet n'échappera pas à Genève. L'Office fédéral de la communication conteste cette vision des choses: «A une époque où les positions dans le domaine de la gouvernance numérique se durcissent, un lieu neutre comme la Genève internationale revêt une importance croissante. […] Le renforcement de la Genève internationale, en particulier dans le domaine numérique, est donc un objectif central de la stratégie Suisse numérique et de la stratégie de politique étrangère 2020-2023 récemment adoptée.»

3. Commentaire d’Alain Empain sur l’article précédent

20200411

Un pays qui a le monopole techno-logique et de la (dés)information va certainement tout faire pour ne pas le perdre.

On a déjà bien vu jusqu'où ils sont capable d'aller pour interdire aux pays tiers de choisir autre chose que l'infrastructure de ce monopole (CISCO et al.), dont les 'back doors' officieusement officielles ont été

documentées. Grosses pressions diplomatiques et rétorsions économiques contres les pays amis qui osent regarder autre part... même faire emprisonner une directrice importante de Huawei par un pays ami (Canada) sur prétexte : un peu comme si on emprisonnait Bill Gates de passage à Bruxelles pour des raisons de lutte économique.

On ne sait pas grand chose de la proposition technique, sauf qu'il faut penser et préparer une évolution des protocoles : par principe c'est assez légitime. Dans le passé cette mise au point et évolution a été faite de manière exemplaire (les fameux RFCxxx 'Request for Comments', un modèle de

l'esprit d'ouverture de l'information, qui a donné la culture opensource).

Il est bien possible que les critiques de l'article soient valables, à condition de bien être attentif à ne pas faire gratuitement un procès d'intention par inversion [accuser les autres de ce qu'on fait] de ce qui est concocté par le monopole de fait actuel : les chinois peuvent bien entendu avoir des intentions antidémocratiques, mais ceux qui critiquent feraient bien de se regarder dans le miroir.
Les documents fuités par Snowden démontrent bien, sans ambiguïté, qu'au niveau intentions et technicité, les USA

feraient bien de ne pas trop faire de vagues.

L'idéal pour moi serait de prendre la proposition chinoise et de la mener à la manière des RFC afin de veiller à la garantie d'ouverture et de sécurisation par rapport aux interférences étatiques et des dérives possibles ou probables.

Sans s'occuper des cris d'orfraies de ceux qui aimeraient bien le faire mais à leur avantage seul, car eux vont essayer de dévier la discussion par n'importe quel moyen et accusation.

4. Inside China's controversial mission to reinvent the internet

Madhumita Murgia & Anna Gross, FT, with Yuan Yang and Nian Liu

20200327

Current Source: https://dnyuz.com/2020/03/27/inside-chinas-controversial-mission-to-reinvent-the-internet/

Original source: https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f

On a cool day late last September, half a dozen Chinese engineers walked into a conference room in the heart of Geneva’s UN district with a radical idea. They had one hour to persuade delegates from more than 40 countries of their vision: an alternative form of the internet, to replace the technological architecture that has underpinned the web for half a century.

Whereas today's internet is owned by everyone and no one, they were in the process of building something very different — a new infrastructure that could put power back in the hands of nation states, instead of individuals.

The team who had masterminded the New IP (internet protocol) proposal was from the Chinese telecoms giant Huawei, which had sent the largest delegation of any company to the September meeting.

At the gathering, held at the International Telecommunications Union, a UN agency that establishes common global standards for

technologies, they presented a simple PowerPoint. It didn’t bother with much detail on how this new network would work, or what specific problem it was solving. Instead, it was peppered with images of futuristic technologies, from life-size holograms to self-driving cars.

The idea was to illustrate that the current internet is a relic that has reached the limits of its technical prowess. It was time, Huawei proposed, for a new global network with a top-down design, and the Chinese should be the ones to build it.

Governments everywhere seem to agree that today’s model of internet

governance — essentially, lawless self-regulation by private, mostly American companies — is broken.

New IP is the latest in a series of efforts to change the way the internet is run, spearheaded by governments that were largely left out when it was founded half a century ago. “The conflicts surrounding internet governance are the new spaces where political and economic power are unfolding in the 21st century,” wrote the academic Laura DeNardis in her 2014 book The Global War for Internet Governance.

The Chinese government in particular has viewed designing internet

infrastructure and standards as core to its digital foreign policy, and its censorship tools as proof-of-concept for a more efficient internet, to be exported elsewhere.

“Of course [China] want a technological infrastructure that gives them the absolute control which they have achieved politically, a design that matches the totalitarian impulse,’’ says Shoshana Zuboff, author of The Age of Surveillance Capitalism and a social scientist at Harvard University. “So that is frightening to me and it should be frightening to every single person.”

Huawei claims that New IP is being developed purely to meet the technical requirements of a rapidly evolving digital world, and that it has not yet baked a particular governance model into its design. The telecoms giant is leading an ITU group that is focused on future network technology needed by the year 2030, and New IP is being tailored to meet those demands, a spokesperson says.

What is known about the proposal has come primarily through two jargon-filled documents that have been shared with the FT. These were presented behind closed doors to ITU delegates last September and this February. One is

a technical standards proposal, and the other a PowerPoint titled “New IP: Shaping the Future Network”.

Despite the might of today’s internet, it has no regulator; instead, power is largely held by a handful of US corporations — Apple, Google, Amazon, Facebook. This lack of central oversight is the very thing that has allowed technologists to transform how we communicate and live but it has also enabled deep fractures in our social order, including the manipulation of public dialogue, the disruption of democracy and the rise of online surveillance.

Today, in the wake of scandals from Cambridge Analytica to the role of Facebook in inciting real-world violence in Myanmar, many experts see the internet as a civic space that requires better public hygiene. Governments — whether democratic or authoritarian — are tired of being shut out and are agitating for more influence online.

The power balance is starting to shift but the scope of what states want varies widely. The US, UK and Europe, for example, are interested in adapting the current system to introduce more regulatory power, and give intelligence agencies greater access to users' personal data.

The Chinese New IP proposal is far more radical, and could embed a system of centralised rule enforcement into the technical fabric of the internet. Saudi Arabia, Iran and Russia have previously shown support for Chinese proposals for alternative network technologies, according to sources who were present at ITU meetings. The proposals revealed that the blueprints for this new network have already been drawn up, and construction is under way. Any country will be free to adopt it.

“Right now we have two versions of the internet — a market-led capitalist version based on surveillance, which is

exploitative; and an authoritarian version also based on surveillance," Zuboff says. "The question is: will Europe and North America pull together to construct the legal and technological frameworks for a democratic alternative?"

The New IP presentation paints a picture of a digital world in 2030 where virtual reality, holographic communication and remote surgery are ubiquitous — and for which our current network is unfit. Traditional IP protocol is described as "unstable" and "vastly insufficient", with "lots of security, reliability and configuration problems".

The documents suggest a new network should instead have a “top-to-bottom design” and promote data-sharing schemes across governments “thereby serving AI, Big Data and all kinds of other applications”. Many experts fear that under New IP, internet service providers, usually state-owned, would have control and oversight of every device connected to the network and be able to monitor and gate individual access.

The system is already being built by engineers from “industry and academia” across “multiple countries”, Huawei’s team lead Sheng Jiang told the group in September, although he would not

reveal who these were due to commercial sensitivities. Among the audience were veterans of the ITU, including mainly government representatives from the UK, the US, Netherlands, Russia, Iran, Saudi Arabia and China.

For some participants, the very idea is anathema. If New IP was legitimised by the ITU, state operators would be able to choose to implement a western internet or a Chinese one, they say. The latter could mean that everyone in those countries would need permission from their internet provider to do anything via the internet — whether downloading an app or accessing a site — and

administrators could have the power to deny access on a whim.

Rather than a unified world wide web, citizens could be forced to connect to a patchwork of national internets, each with its own rules — a concept known in China as cyber sovereignty.

Recent events in Iran and Saudi Arabia provide a glimpse of what this would look like. These governments blacked out global internet connectivity for prolonged periods during civil unrest, allowing only restricted access to essential services such as banking or healthcare. In Russia, a new “sovereign internet” law passed in November

enshrined the government's right to monitor web traffic closely and showed the country's capability to cleave off from the global web — a capability that Chinese companies including Huawei helped the Russians build.

Experts now debate whether China's vision of its internet governance may be shifting from a defensive one, in which the government wished to be left alone to impose authoritarian internet controls at home, to a more assertive approach, in which the country is openly advocating for others to follow its lead.

The creators of New IP say that parts of the technology will be ready to be tested

by next year. Efforts to persuade delegations of its value will culminate at a major ITU conference due to be held in India in November. To persuade the ITU to approve it within the year, so it can be officially “standardised”, representatives must reach an internal consensus, based loosely on majority agreement. If the delegates are unable to agree, the proposal will go to a closed-door vote in which only member countries can participate, cutting out the views of industry and civil society.

This rapid timeline is causing western delegations particular anxiety and demands have been made to slow the process down, according to documents

seen by the FT. One participant from the Dutch delegation wrote in an official response, leaked to the FT by multiple sources, that the “open and adaptable nature” of the internet — both its technical structure and how it is governed — was fundamental to its success and that he was “especially concerned” that this model veered away from that philosophy.

Another stinging rebuke from a UK delegate, also leaked to the FT, declared: “It is far from clear that technically sound justifications have been made for taking such a radical step. Unless these are forthcoming, reasonable foundations for future work

or even continued research activities on these topics are either weak at best, or nonexistent.”

One of the loudest critics of New IP has been Patrik Fältström, a long-haired maverick engineer, known in his native Sweden as one of the fathers of the internet. In the early 1980s, Fältström was a mathematics student in Stockholm when he was hired to build and test the infrastructure for a new technology that the US government was calling the internet.

His job was to write a series of protocols that allowed computers to send text between each other. “In

Europe, we were maybe 100 people in Sweden, 100 in the UK, 50 here, 20 there, all of us knew each other. We used to joke that if there was a problem, you knew who to call," he says.

Today, Fältström is a digital adviser to the Swedish government and its representative at most major internet standards bodies including the ITU. Thirty years after he helped assemble the building blocks of the internet, he embodies the cyber-libertarian western ideals that were woven into its foundation.

"Internet architecture makes it very, very hard, almost impossible for

whoever is providing internet access to know or regulate what the internet access is used for," he says. "That is a problem for law enforcement and others, who would like to have an internet service provider controlling it, so it is not used for illegal activities like pirating movies, or child abuse.

"But I am prepared to accept that there will be criminals who do bad things and police will have an inability to fight [all of] it. I accept that sacrifice."

For Fältström, the beauty of the internet is its "permissionless" nature, as demonstrated during the Arab spring. "We have to remember," he says, "it is a

balance between being able to communicate and control, but people having a voice is always more important.”

A stark contrast to this view can be found in a river-village called Wuzhen near Shanghai, which is emptied out every autumn to make room for the tech executives, academics and policymakers attending the ambitiously named World Internet Conference. The event was created by the Cyberspace Administration of China in 2014, a year after President Xi Jinping rose to power. A row of world flags greets visitors — a nod to Xi’s vision of creating “a

community of shared future in cyberspace”.

Tech executives from Apple’s Tim Cook to Qualcomm’s Steve Mollenkopf have spoken there, lending credence to Xi’s attempts to assemble the international tech elite. But in recent years, foreign attendance has dropped off as the US-China tech war intensifies and executives worry about being too closely aligned with Beijing.

There is precedent for such fears. In the event’s first year, organisers slipped a draft joint statement under guests’ hotel doors at midnight, setting out Xi’s view of each nation’s right to “cyber

sovereignty”. Guests were told to get back with any changes before 8am. After protests, the organisers dropped the matter entirely. But the fact that the leadership had tried such a stunt reflected Xi’s digital ambitions.

In the early 1990s, the Chinese government started developing what is now known as the Great Firewall, a system of internet controls that stops citizens from connecting to banned foreign websites — from Google to The New York Times — as well as blocking politically sensitive domestic content and preventing mass organising online.

Beijing’s technical controls are supported by large teams of government censors as well as those hired by private tech companies such as Baidu and Tencent. Although anyone anywhere in the world can technically host their own website using just a computer and an internet connection, in China one needs to apply for a licence to do so. Telecoms providers and internet platforms are also required to aid the police with the surveillance of “crimes”, which can include actions such as calling Xi a “steamed bun” in a private chat group, an act punished by two years in prison.

Despite this, the Chinese internet is not 100 per cent effective at blocking

content considered sensitive or dangerous by the government. “The leaky global internet remains frustrating for Chinese censors, and they’ve dealt with it at great expense and effort, but if you could make those problems go away almost completely by using a more automated and technical process, perhaps like New IP, that would be fantastic for them,” says James Griffiths, author of The Great Firewall of China: How to Build and Control an Alternative Version of the Internet.

“Building a new version of the internet would potentially block more people from gaining politically dangerous knowledge, saving a huge amount of

effort, money and manpower from the censorship side. They can pick and choose what controls they want, bake it into the tech and roll it out.”

Establishing a sophisticated alternative to the western internet would also fit with China’s ambitions to extend its digital footprint globally. “In the early days of the internet, China was very much a follower and didn’t recognise, like many other countries, how disruptive the internet would be,” says Julia Voo, research director for the China Cyber Policy Initiative at Harvard University’s Belfer Center.

“As they realised how important it was, [they] funnelled more resources into developing technologies . . . and we can see their increased influence in many standards organisations like the ITU in the past two or three years.

“But the US and others have made a strategic mistake in not seeing the value of growing infrastructure in developing markets,” she adds. “There is still a lot of infrastructure that needs to be provided and in the past 10 years it has been Chinese companies that have been the ones to provide it, particularly in Africa.”

Beijing has signed memoranda of understanding on building a “Digital Silk Road” — or system of advanced IT infrastructure — with 16 countries. Huawei says it has 91 contracts to provide 5G wireless telecoms equipment worldwide, including 47 from Europe — despite US warnings that Huawei’s involvement was tantamount to giving the Chinese access to national security secrets, an allegation rejected by the company.

“In proving that you can control and intensely surveil your domestic internet and avoid it being used as a tool to rally people against the government, combined with the economic success of

its companies, China has made this vision incredibly attractive to regimes — autocratic and otherwise — around the world," says Griffiths.

The ITU was created 155 years ago, making it one of the oldest international organisations in the world, predating even the UN. It is housed in a set of glass-panelled buildings in Geneva's Place des Nations. On the 10th floor of one is the airy office of Bilel Jamoussi, the Tunisian-born head of the ITU's study groups — the units that develop and ratify technical standards.

The room is lined with an enormous bookcase from which Jamoussi pulls a

dusty blue book — his PhD thesis, penned 25 years ago, about traffic going through the internet. At the time, there was a desire to build a new networking protocol to meet the internet's growing user base. In the end engineers opted to layer on top of the existing TCP/IP infrastructure. The technology, invented in the late 1970s by computational engineers working for the US defence department, was a way of transmitting messages between computers at the speed of light, using a special addressing system.

"Twenty-five years ago we had this conversation as a community — is it TCP/IP or is it something else — and

then a lot of design and development happened to kind of rescue [it],” Jamoussi says. “We are now, I think, at another turning point, of saying, is that enough, or do we need something new?”

In its earliest days, the ITU oversaw the first international telegraph networks. Since then, it has grown from 40 nations to 193 and has become the de facto standards body for telecoms networks. Standards produced there legitimise new technologies and systems in the eyes of certain governments — particularly those in the developing world who don’t participate in other internet bodies. Ultimately, they give a

commercial edge to the companies who have built the tech they are based upon.

Over the past 21 years, Jamoussi has witnessed a geopolitical shift. “The pendulum has swung to the east, and now we see more participation from China, Japan, Korea,” he says. “Twenty years ago it was Europe and North America that were dominating the products, solutions and standards development, now we have a swing to the east.”

On one of the ITU’s marble walls, backlit flags are hung, showing the biggest donor nations. The Chinese flag — currently at number five — was not

there at all a few years ago, an employee explained, but it has been gradually working its way up.

New IP is the latest grenade thrown into the ITU's arena, but it is hardly the first internet-related standard to be proposed as an alternative to the original western-designed system. The governments of Russia, Saudi Arabia, China and Iran have been pushing the idea of alternative networks for years, according to participants who wished to remain anonymous.

"In the early 2000s, once you saw widespread take-up of the internet, suddenly you had this idea of

democratisation, of essentially giving people more control and more information. For authoritarian governments, that was something they weren't happy with," says one member of the UK delegation. "And so work started, around the early 2000s, particularly in China, and then a bit later in Iran and Russia, around how to create an alternative to the standards and the technologies that were being developed mostly by Americans still."

But in recent years, Chinese companies have moved on to New IP. "There's a new paradigm, it's not voice and text and video and people chatting, it's the real-time controlling of something

remotely, or having telepresence, or holograms," Jamoussi explains. "Those new applications are requiring new solutions. And now it's more feasible, it's no longer science fiction, it's close to being a reality."

Spearheading plans for New IP is Richard Li, chief scientist at Futurewei, Huawei's R&D arm located in California. Li has been working with Huawei engineers based in China, as well as state telecoms companies China Mobile and China Unicom, with the explicit backing of the Chinese government, to develop the technology specifications and standards proposal.

Having Huawei at the helm will ring alarm bells for many in Europe and the US, where governments have become concerned that Chinese technology is being developed as a vehicle for state espionage. The advent of 5G — a much higher bandwidth network which will serve as the digital spine for a more automated world — has led to rising concern that products developed by Huawei will be built with “back doors” for spies in Beijing.

Last year, the US blacklisted Huawei from selling into its market, and the UK government is embroiled in a parliamentary battle over the company’s

involvement in its core telecoms infrastructure.

The FT reached out to Li to discuss New IP, but Huawei declined the opportunity for him to explain the idea in greater detail. The company said in a statement: “New IP aims to provide new IP technology solutions that can support . . . future applications such as Internet of Everything, holographic communications, and telemedicine. The research and innovation of New IP is open to scientists and engineers worldwide to participate in and contribute to.”

Critics argue that the technical claims made in the New IP documentation are either false or unclear, and represent a “solution looking for a problem”. They insist that the current IP system is fit for purpose, even in a rapidly digitising world. “The way that the internet has developed is through building blocks that are modular and loosely coupled, that’s the brilliance of it,” says Alissa Cooper, chair of the Internet Engineering Task Force (IETF), an industry-dominated standards body in the US.

In November, Li presented to a small group during an IETF meeting in Singapore, which Cooper attended.

“[The current infrastructure] is in pretty stark contrast to what you see in the New IP proposal, which is this kind of monolithic, top-down architecture that wants to tightly couple the applications to the network. This is exactly what the internet was designed not to be,” she says.

The implications for the average user could be enormous. “You’re pushing control into the hands of [telecoms] operators which are state-run,” says a UK ITU delegation member. “So [it means] you can now not only control access to certain types of content online, or track that content online, but you can

actually control the access of a device to a network.”

China is already in the process of building a credit-scoring system for its population, based on online and offline behaviour and past “misdemeanours”, the delegation member noted. “So if somebody’s social credit score dipped below a certain amount because they were posting on social media too much, you could actually prevent that phone from connecting to the network.”

China’s telecoms operators have a wealth of data on their subscribers. By law, customers have to register for a phone number or internet connection

using their real name and identification, which is then accessible by other companies such as banks. The country's cyber-security law also mandates that all "network operators", which includes telecoms companies, must keep "internet logs" — although it is not clear what these entail.

Jamoussi argues it is not the ITU's place to judge whether proposals for a new internet architecture are "top-down'" or could be misused by authoritarian governments. "Of course anything you build, it's a two-edged sword. You can use anything for good or for bad, and it's the sovereign decision of every member state," he says. "In the ITU we

don’t go into that potential misuse of technology, we just focus on, ‘here is some . . . communication technology problem, here is an aspiration, let’s as a community build a solution to reach that.’ But then how people use it is really up to them.”

Beijing’s ambitions to build more controls into the internet infrastructure are not seen as a problem by everybody — merely as the next chapter in its evolution.

“The internet was supposed to be a neutral infrastructure, but it has become a politicised arm of control. Increasingly internet infrastructure is

being used for policy goals — to repress people economically, and physically — we saw it in Kashmir, Myanmar and in the Snowden revelations," says Niels ten Oever, a former Dutch delegate at the ITU.

"For me, the overarching question is: how do we build a public network on privately owned infrastructure? This is the problem we are grappling with. What is the role of the state versus the role of companies?"

In his view, companies design technologies primarily for profit. "The internet is dominated by US companies, all data flows there. So, of course, they

want to keep that power," he says. "We are scared of Chinese repression. We are making caricatures of the Chinese in a borderline imperialist-racist way. But the internet governance today is not working. There is room for an alternative."

Wherever our digital future is currently being built, there seems to be global agreement that the time has come for a better version of cyberspace. "I think [some] people would argue that our current model of the internet is deeply flawed, if not broken. At present, there is only one other truly comprehensive and fully realised model out there,

China's," wrote Griffiths in The Great Firewall of China.

"The risk is that if we fail to come up with a third model — one that empowers users and increases democracy and transparency online, and reduces the powers both of big tech and government security services — then more and more countries will tilt towards the Chinese model, rather than deal with the fallout of the failing Silicon Valley one."

Today, the "Declaration of the Independence of Cyberspace" — the guiding principle of the internet — is starting to look more and more like a

relic. The manifesto, written in 1996 by John Perry Barlow, co-founder of the American non-profit Electronic Frontier Foundation, and a Grateful Dead lyricist, was a call to arms.

“Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind,” starts the document. “On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.”

That view has now become a throwback to a time before trillion-dollar market capitalisations in the tech industry,

critics say. But there is still hope — and possibly a third alternative to our two internets of today.

“What differentiates us from China now is that in the west, the public can still mobilise and have a say. A lot of this now is down to lawmakers to protect democracy in an age of surveillance, whether it’s market-driven, or authoritarian-driven,” says Zuboff. “The sleeping giant of democracy is finally stirring, lawmakers are waking up, but they need to feel the public at their backs. We need a western web that will offer the kind of vision of a digital future that is compatible with

democracy. This is the work of the next decade.”

Madhumita Murgia is the FT’s European tech correspondent. Anna Gross is an FT markets reporter. Additional reporting by Yuan Yang and Nian Liu

5. The Geopolitics of Data

Abishur Prakash, Geopolitical Futurist, Center for Innovating the Future, Canada

20191205

Source: https://medium.com/henley-partners/the-geopolitics-of-data-26d1ab708678

What would you do if you wanted to travel to Germany but couldn’t buy an airline ticket because you had a low social score? If you haven’t heard of the term “social score” perhaps you should travel to China. In 2018, more than 9 million Chinese individuals were blocked from booking flights because their social scores were too low. Their scores were derived from their online activity, spending habits, and political party loyalty. While this may sound peculiar to some, what is happening in China reflects just one way in which data is now being tapped.

Could Data Prompt Clashes between Japan and Thailand?

Over 700 million people around the world use Line, a Japanese messaging app. In 2019, Line launched a new feature called Line Score, which uses algorithms to give users a score calculated based on the data a user produces (their activity across the different Line services). Depending on their score, a user will be able to access various Line services. For example, Line Pocket Money, which offers app users loans, is in the process of determining how much credit a user can get based on their Line Score. By giving

users a score, Line is changing the role of business in the lives of individuals; the firm is transitioning from a private company to a digital government that punishes and rewards people based on their activity data.

How might this affect geopolitics in Asia? In the coming years, Line might look to explore the Thai market, subsequently finding itself in a position of being able to ‘shape’ the lives of locals. To illustrate, if an individual needs a job, a loan, investment options, or insurance they may very well consider Line products. In turn, the app could use Line Score to determine what

Thai clients can access, posturing Line inadvertently to govern the lives of people in Thailand thanks to access to vast amounts of data and complex algorithms. Would the Royal Thai Government be comfortable with this, or might it view Line processes and strategy as being a new kind of colonization via data?

In case of the latter, the Royal Thai Government might decide to cut off the supply of data to Line in an effort to sap the app's potential stronghold, meaning Line would no longer have access to data from Thai banks and/or retailers. This would likely create chaos for

Line’s business lines and may force Japan to intervene to protect its technology company. Consider what is happening here: Line’s new business model is essentially a social design that has the very real potential to take away power from the Royal Thai Government and spark tensions between the governments of Thailand and Japan. For the first time, a private company may cause two governments to clash because of data. As for Japan, how might she respond? Perhaps Japan could threaten to shut off all Japanese robots operating in Thailand, bringing the Thai manufacturing sector to a halt, or Japan

could direct all of its artificial intelligence (AI) firms to stop hiring Thai engineers and programmers.

There is also the role that the Association of Southeast Asian Nations (ASEAN), of which Thailand is a member state, could play, possibly involving the entire region in the inter-state conflict. If ASEAN feels that one of its members is being influenced by the Japanese algorithms, it could threaten trade or diplomatic action against Japan. ASEAN may do this not just to support Thailand but to also send a message to the world that creating problems with ASEAN members may

prompt the intervention of the intergovernmental organization.

It is also worth considering the broader ecosystem that may be reliant on Line Score. For example, banks in the Middle East may be providing local clients financing for loans through Line. Or, insurance firms in the USA may be providing health and auto protection through Line. If Line Score is affected in Thailand, the entire ecosystem may be adversely affected. Could this spur other governments to step in? Could Line or Thailand have imagined that a regional issue over data could become so global?

Could Public Policy around Data Fuel New USA Power?

As world powers compete over technologies like AI, data is becoming one of the keys to gaining an advantage. Without data, companies — and countries for that matter — can’t fuel their AI systems. With data, however, AI can advance to new levels, meaning that public policy around data is becoming a new geopolitical flashpoint.

Take the USA and India. In 2018, India proposed a new set of laws that would compel technology companies collecting data in the country to store that data therein (data localization). As

technology companies held their breath, the USA government intervened. In 2019, the USA warned India that if data localization laws came into effect, the USA could reduce the number of H-1B visas it grants to people from India. For the first time in history, the data laws of one country are affecting the immigration policy of another country, and caught in the middle are technology companies ‘merely’ wanting to expand their commercial footprint through India’s market. Significantly, the data laws that India is considering today may be nothing compared to what is to come. Niti Aayog, India’s government

think tank, has proposed creating an open marketplace where companies share their data. Companies of all sizes, foreign and domestic, would be required to share their data so everyone can benefit, including competitors — meaning USA firms could lose their competitive edge in India.

How might the USA respond to this move? While the country would have to weigh the importance of data with other parts of its relationship with India, such as weapons sales, it may be spurred to take a particular course of action in light of how other countries react to India's data laws, such as China for example.

Weeks before the USA threatened using H-1B visas, the government of China announced that it would comply with India's data localization ruling.

Heads of state of ASEAN nations gathered at the 33rd ASEAN–Republic of Korea Summit held in Singapore in 2018

Instantly, multiple geopolitical shifts are taking place. Firstly, India's laws are pressuring USA–India ties. Secondly,

the laws appear to be bringing India and China closer. These two shifts — pressure on USA–India ties and closer India–China ties — may impact on a third set of relations: USA–China ties. If USA businesses lose access to foreign markets because of public policy while Chinese companies succeed, it could anger the USA government. In turn, the USA may double down on current sources of tension, such as trade, intellectual property, or currency devaluation as a way to strike back at China. In other words, how China and the USA comply with public policy in India could begin to impact on the

geopolitics between Beijing and Washington. Thirdly, private companies from the USA and China are being restricted by how their respective governments are reacting to India's data laws. Will they listen? The USA government may be able to control companies from traditional sectors, such as defense or investment banking, but technology companies, many of whom have government-like power, may ignore or reject the USA rulings or desires. What this means is that for the first time, because of technology, companies could have a different

foreign policy than the country they originate from.

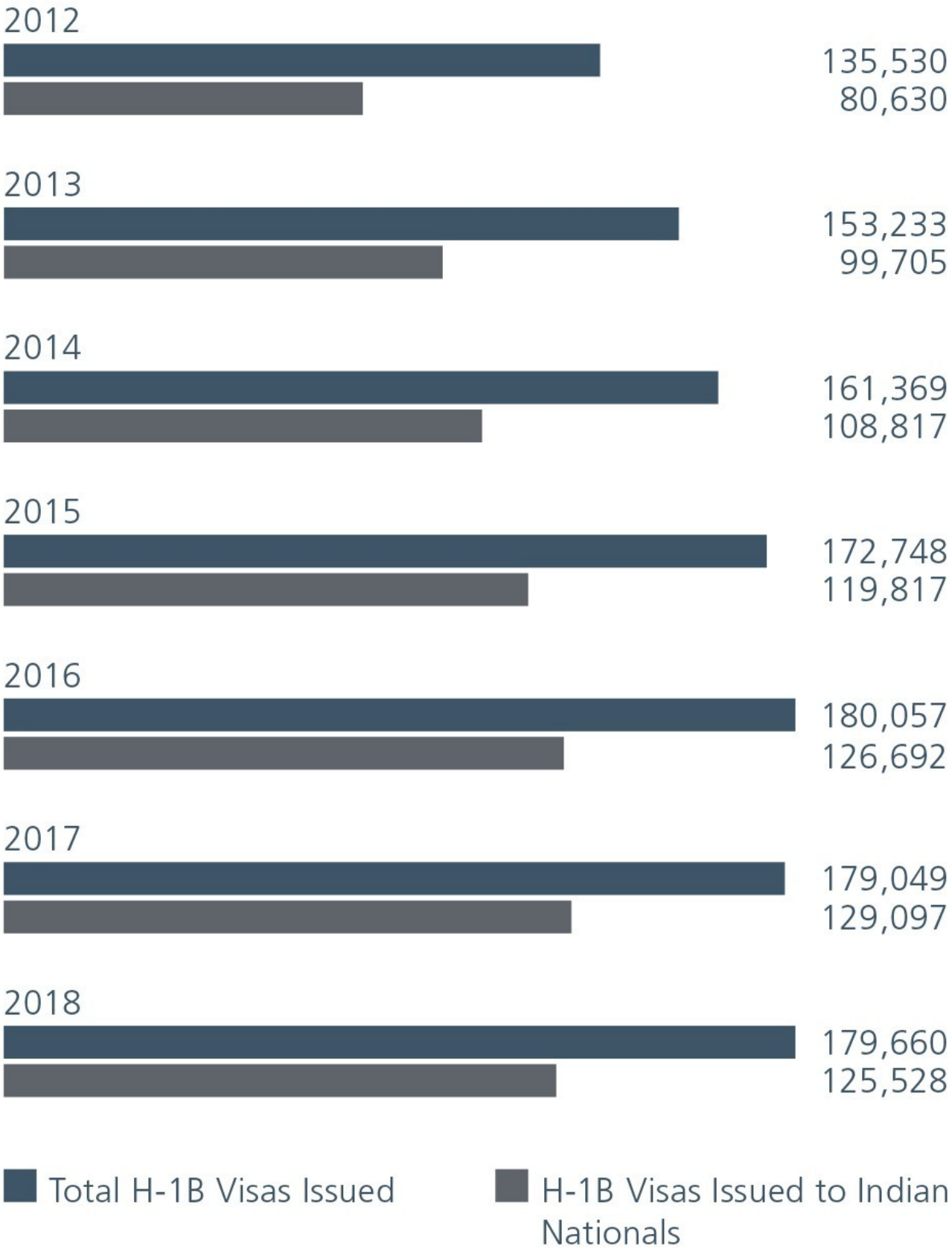
If the USA feels outplayed in India and other markets because of data laws, it might take a different route to enforce its will. Could it introduce the world's first Data Trade Organization (DTO), tasked with prescribing global rules for data? By forming the first DTO, the USA may be in charge of creating the rules, laws, and protocols that govern data use from San Francisco to Shanghai to Sydney. Just like the World Trade Organization, which gave the USA power over trade, so too could the

DTO give the USA significant power over data. What this means is that while India may control where companies store data (i.e. in India), the USA may control how that data can be used. What's more important — where data is stored or how data is used?

This would be a new strategy through which to reconfigure USA geopolitical power through data. For the first time, nations may 'feel' the presence of the USA not through warships or corporations but by complying with data rules set in Washington. Of course, this assumes India and other countries

join the USA’s DTO. If not, could they create their own data bloc?

Allocation of H-1B Visas Issued to Indian Nationals



(Source: *The Economic Times*, July 2019)

Will Data Begin to Control People?

Until recently, companies and countries collected data for a handful of reasons: some brands collect data to boost sales through hyper-personalized ads, while some governments collect data to identify national security challenges such as terrorism. These uses come with major privacy implications but, for the most part, the way data is collected and used today does not limit what someone can or cannot do. Soon things may be different however.

For example, the UK is experimenting with citizen scores. More than 50 councils throughout the UK have spent

a combined GBP 2 million to buy AI that crunches data, divides people into different groups, and allocates them a score. Then, the software makes predictions about ‘future outcomes’. For example, the AI analyzes variables like martial status, socio-economic status, family members, and financial information to divide households into different categories. Then, the AI uses this analysis to predict possibilities such as whether one area will be at higher risk of alcohol addiction. Governments then use these predictions to formulate policy.

This represents a new kind of society that is emerging. For the first time, the data that someone produces — from commenting online to paying bills late — could end up controlling them in ways previously unimagined. The New Zealand government is experimenting with algorithms that look at data and predict whether a new immigrant is likely to commit crime. Based on these predictions, the immigration agency can then decide whether to arrest an immigrant, extend their visa, or even deport them. The ethical implications of this are enormous. Governments are starting to view people through the

predictions and assessments that algorithms produce. The human element is disappearing.

This may end up creating a new geopolitical challenge for Wellington. The next generation of immigrants may decide not to move to New Zealand because of the algorithms. And, if these algorithms are biased, it might deter immigrants even more. If fewer people immigrate to New Zealand, new opportunities may unveil for other nations. For example, as people ignore New Zealand, the UAE might reach out to countries and begin to market the UAE as a data-neutral zone. What this

means is that the data people produce in the UAE may not be used against them, unlike in New Zealand.

Things become more confusing when considering the ‘other’ kinds of data that are being collected and used. In the USA, a firm called Genomic Prediction is applying machine learning algorithms to huge sets of genomic data. Based on this analysis, the firm hopes to predict the cognitive abilities of embryos. In other words, the firm wants to determine how smart a child will be before the child is born. If such technology is adopted, it will fundamentally change the world. For

example, in order to grow its economy, Brazil could implement predicting the intelligence of future generations and assign people jobs before they are born. This means that private companies may be working with governments to decide where people can work before those people have even arrived.

Governments may create economic plans 10 or 20 years in advance based on the predicted intelligence of future populations. This extreme use of data carries enormous ethical and moral consequences. It means that for the first time the world will be judging how

valuable somebody is before they even see first light. Are people ready for this?

Why is data now so powerful when until recently it was essentially just a mirror for society? As people produced data, they were also producing a digital picture of themselves. Through this picture, somebody could understand how a person thought, felt, and ultimately, who that person was. This is what has made social media so valuable and is what has made surveillance so scary. Data is now no longer just about people: it is also about geopolitics. Thanks to data, new social designs are emerging, transforming countries from

Europe to Asia. At the same time, how governments regulate and control data within their borders is affecting global relationships. All of this means that local and global are being connected in ways that have not existed before.

USA tech firms including the likes of Amazon, Google, and Microsoft are among the leading employers of H-1B applicants. Seen here are Amazon employees at the firm's largest campus building in Hyderabad

A photo that someone posts in Taipei, a message that somebody sends in Munich, a video that somebody uploads in Dubai are no longer disconnected from each other. They all are connected and carry major geopolitical consequences. The geopolitics of data then, is not actually about data at all. Rather, it is about people and the choices they are making every single day — all of which is being tracked, collected, and analyzed through complex algorithms. For the first time, people are part of geopolitics in a way they have never been, and that means the next time you see someone taking

out their phone, buying a cup of coffee, or making a purchase at a retail store, remember that what they are doing is producing data that may play a small part in shifting global power and changing societies in all four corners of the world.

6. Governments are erecting borders for data

Data sovereignty is rapidly becoming a big issue

The Economist

20200220

Source: https://www.economist.com/special-report/2020/02/20/governments-are-erecting-borders-for-data

SOMEWHERE DEEP in the bowels of Microsoft’s campus in Redmond near Seattle, a jumble of more than 100 buildings, there is a special kind of room. The size of a school gym, its walls are covered with big screens. One shows the “health” of the firm’s cloud-computing services, collectively called Azure. Another displays people’s “sentiment” about the system, as expressed on social media. A third one, a large map of the world, tells visitors how many “denial-of-service” (DOS) attacks, which amount to flooding a customer’s online presence with bits to shut it down, are currently being dealt

with. The counters on this Thursday morning in early December show 80 in Asia, 171 in Europe and 425 in the Americas.

It would be fair to assume that the room is a NOC, a “network operations centre”, to manage Azure. But nothing gets controlled here; that happens elsewhere. Instead, the room, called the Cloud Collaboration Centre (CCC), serves two other purposes. One is, in the words of Anja Ziegler, who manages the location, to “put a face on the cloud”—giving customers an idea what Azure and the mirror worlds it powers are about. But more important, the room

serves as a place for Microsoft employees to discuss how to reshape the cloud in response to legal changes in the data economy.

One of the first projects to be tackled in the CCC was how to make Azure compatible with the General Data Protection Regulation (GDPR), the EU’s tough privacy law that went into effect in 2018. The room has only become busier since: privacy and other data-related legislation is multiplying around the world. Sometimes virtual borders need to be erected, so that data do not leave or enter a certain country. Or a new data centre needs to be built to

give the digital stuff a local home. If this trend holds, Microsoft may soon have to upgrade the CCC's world map —to show the planet's many different data zones, rather than just DOS attacks.

The CCC is thus a place where another tension of the data economy is playing out. Data were supposed to float freely around the world to where they are most efficiently crunched. But flows are increasingly blocked by governments which seek to protect their country's people, sovereignty and economy. And these first rustlings of digital protectionism, predicts Ian Hogarth, a noted British entrepreneur and writer,

could turn into fully fledged “AI nationalism”, as countries go beyond just defending their data assets and try to build a data economy of their own.

Just as with the internet itself, there were not supposed to be any trade-offs in the cloud. The “cosmopolitan ideal” was that the free flow of data would make the world if not a better place, at least a more efficient one, observes Andrew Woods of the University of Arizona, who is writing a book about data sovereignty. It would allow digital stuff to end up in data centres located in places near many users, with lots of connectivity and where land and energy

are cheap and the air cool and dry. (Cloud data centres can be several football fields large and consume huge amounts of energy, about half of which is used for cooling.)

Whose cosmopolitan ideal?

In practice this has meant that the biggest clouds have risen over America, which so far has set the rules of the data economy. It not only boasts the biggest and most innovative tech companies, but plenty of potential customers, fibre-optic cables, cheap power and land to build cavernous data centres. To get an impression of the concentration of computing power in America, one need

only drive a few hours east of Microsoft's campus to Quincy, Washington, a town with a population of not even 8,000. This is home to two dozen large data centres, many operated by Microsoft.

As long as computing clouds were small, this uneven distribution did not matter much. But, starting with the intelligence leaks by the American security expert Edward Snowden in 2013 which revealed widespread snooping by America's spy agencies, governments have begun to understand the importance of this global infrastructure—and, by extension, the

data economy. Citizens' privacy is not the only worry. Data may also reveal things about a country's defences. If digital evidence is stored abroad, law enforcement might be inhibited. Data should be kept close, some governments think, lest other countries benefit from them.

As a result, in recent years virtual borders have been going up in the digital cloud. The GDPR allows personal data to leave the EU only if firms have appropriate safeguards in place or if the destination country has "an adequate level of protection". India blocks payment information from

leaving the country and may soon require that certain types of personal data never leave the country. Russia requires that data be processed and stored on servers within its territory. China blocks most international data flows. And the EU is discussing creation of a single market in data, like the one it already has for goods.

These growing and unco-ordinated efforts to regain data sovereignty have already triggered debates at the highest level of international diplomacy. In July the G20, a group of 20 developing and rich countries, launched the “Osaka Track”, named after the Japanese city

where the decision was taken. The idea, which Abe Shinzo, Japan's prime minister, floated early last year is to come up with some global rules for "data governance", guided by the rather fuzzy concept of "free flow of data with trust".

It is still unclear where all this will lead. What will the world map in Microsoft's cloud centre look like a decade hence? Will it resemble today's global maps, showing as many data zones as there are countries? Or will it display a few digital trade zones (known as "data spheres") or something completely different?

The first possibility is rather unlikely. To prevent all data from flowing, countries would essentially have to cut their connection to the internet: it would be the only way to ensure that data really stays put. Russia may be willing to accept the huge economic costs of such a digital secession. But most countries will probably shy away from the drawbacks of even less draconian measures. An overly protectionist country could see cloud-computing providers refuse to serve their market because it is too small. Building a domestic cloud is both tricky and expensive.

The second scenario is far more likely. In fact, this is already happening. Coalitions for different types of data have begun to form. The GDPR's adequacy requirement effectively created one: the need to export personal data from the EU pushed a dozen countries, including America and Japan, to agree to strict data-protection rules. America has started a similar club with the Cloud Act, a bill passed in 2018 to allow the government to negotiate reciprocity agreements with other countries. If these allow American law enforcement to access data stored in partner territory more rapidly than is

possible today, agencies in those countries can get easier reciprocal access, too. Britain has already signed such an agreement; the EU is expected to do so soon.

Although the Osaka Track talks are meant to come up with global rules, they could end up creating another data coalition. The initiative started life as a proposal by the Japanese government to form an alliance with America and the EU to promote the free flow of data between members and to limit access by countries which indulge in data protectionism, notably China. If that is still the agenda, it could push China and

others to create their own data club, warns Justin Sherman of New America, a think-tank. In an early sign of what this may mean, India and a few other developing countries have refused to sign up to the Osaka Track.

The third possible future of the global data sphere is again less likely, but the most intriguing. Somewhat unexpectedly, it is rooted in Germany and comes by the name of GAIA-X, referring to the goddess of Earth in Greek mythology, with the X being a placeholder for future specialisation (GAIA-Health, GAIA-Mobility). Rightly feeling that the country is

behind in cloud computing and risks losing control of its data economy, the German government first considered building something like an “Airbus Cloud”, like a repeat of Europe’s successful aeroplane consortium. Realising that this would probably fail, however, the government has settled on another approach. It hopes to assemble what the Federal Ministry for Economic Affairs calls a “federated data infrastructure”, essentially a club of clouds whose members have to comply with a set of rules and standards.

The main aim is still one of industrial policy: seeding the formation of an

“über-cloud”, a legal-cum-software layer that would insulate German firms and government agencies from the power of big foreign clouds by minimising “lock-in”. Although details have yet to be worked out, it would probably allow firms to move data and computing workloads between rival clouds more easily. GAIA-X could be a tool to implement granular national data policy, instead of resorting to crude digital protectionism. It could help solve the problem of American or Chinese firms dominating the global data infrastructure. The project also includes an initiative called “International Data

Spaces” to make data-sharing between firms and across borders easier.

Yet it is not clear how the German government intends to will this über-cloud into existence, says Stefan Heumann of the Stiftung Neue Verantwortung, a think-tank in Berlin—nor how it does not end up being a lowest common denominator or held up by lengthy negotiations. The plan is to have a “proof of concept” ready by the second quarter of this year, but don’t hold your breath.

Still, the idea may gain momentum. The German government intends to push the concept when it takes over the

presidency of the European Council later this year. France has already signalled support; other countries are expected to join. And some 100 firms and organisations have already joined the effort, including the big cloud providers. The only notable exception, until recently, had been Microsoft. This was a surprise: Azure is the most compatible with Germany's vision. Whether because it has always had many governments as customers or the fact that it does not make money by hoarding data, from the start Microsoft has built its cloud for a world with a

data space fragmented along national lines.

If the vision of GAIA-X comes to pass, how will Microsoft display this on the screens of its CCC? Rather than showing a few data “blocs” in bright colours—China red, America blue, for instance, as during the cold war—it may need lots of shades and other graphic tricks to represent the new diversity of the data world.

7. Who will benefit most from the data economy?

It is already unequal and that inequality could get worse

The Economist
20200220

Source:
https://www.economist.com/special-report/2020/02/20/who-will-benefit-most-from-the-data-economy

THE DATA economy is a work in progress. Its economics still have to be worked out; its infrastructure and its businesses need to be fully built; geopolitical arrangements must be found. But there is one final major tension: between the wealth the data economy will create and how it will be distributed. The data economy—or the "second economy", as Brian Arthur of the Santa Fe Institute terms it—will make the world a more productive place no matter what, he predicts. But who gets what and how is less clear. "We will move from an economy where the

main challenge is to produce more and more efficiently," says Mr Arthur, "to one where distribution of the wealth produced becomes the biggest issue."

The data economy as it exists today is already very unequal. It is dominated by a few big platforms. In the most recent quarter, Amazon, Apple, Alphabet, Microsoft and Facebook made a combined profit of $55bn, more than the next five most valuable American tech firms over the past 12 months. This corporate inequality is largely the result of network effects—economic forces that mean size begets size. A firm that can collect a lot of data, for instance,

can make better use of artificial intelligence and attract more users, who in turn supply more data. Such firms can also recruit the best data scientists and have the cash to buy the best AI startups.

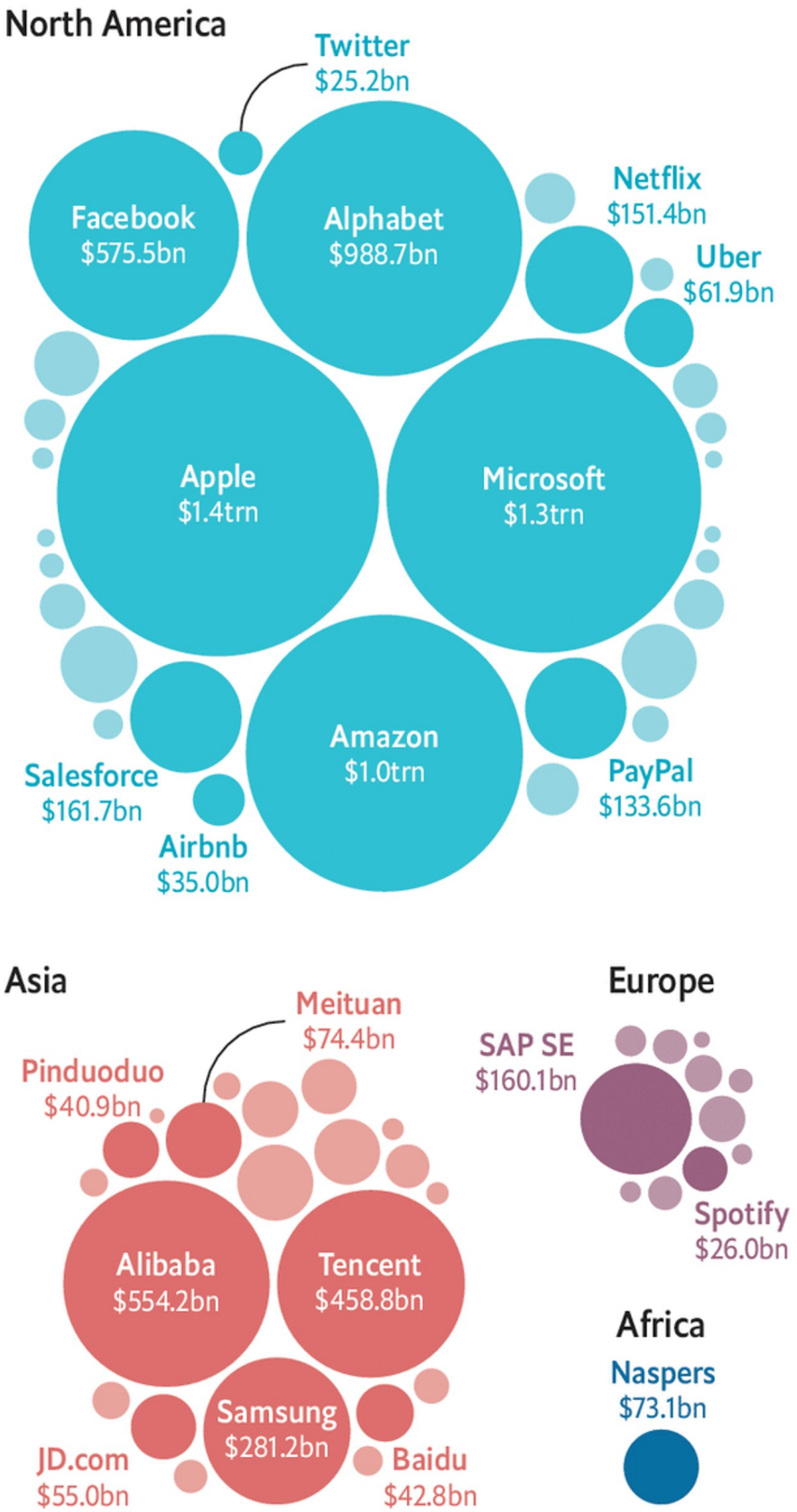
It is also becoming clear that, as the data economy expands, these sorts of dynamics will increasingly apply to non-tech companies and even countries. In many sectors, the race to become a dominant data platform is on. This is the mission of Compass, a startup, in residential property. It is one goal of Tesla in self-driving cars. And Apple and Google hope to repeat the trick in

health care. As for countries, America and China account for 90% of the market capitalisation of the world's 70 largest platforms (see chart), Africa and Latin America for just 1%. Economies on both continents risk "becoming mere providers of raw data...while having to pay for the digital intelligence produced," the United Nations Conference on Trade and Development recently warned.

Two-horse race

Selected global platforms, market capitalisation*

February 1st 2020



Sources: Bloomberg; CB Insights

*Over $3bn

The Economist

Yet it is the skewed distribution of income between capital and labour that may turn out to be the most pressing problem of the data economy. As it grows, more labour will migrate into the mirror worlds, just as other economic activity will. It is not only that people will do more digitally, but they will perform actual “data work”: generating the digital information needed to train and improve AI services. This can mean simply moving about online and providing feedback, as most people already do. But it will increasingly include more active tasks, such as labelling pictures, driving data-

gathering vehicles and perhaps, one day, putting one's digital twin through its paces. This is the reason why some say AI should actually be called "collective intelligence": it takes in a lot of human input—something big tech firms hate to admit.

If history is any guide, the risk is not so much that humans will automate themselves away. Previous technological disruptions have at times even increased labour's share of income, as new types of jobs emerged. The question is rather how much such data workers will be paid. As things stand, their work may become

systematically undervalued, reckons Glen Weyl of Microsoft. One reason is the structure of online markets: big platforms are not just monopolies, but monopsonies, meaning that they have the power to hold down wages for data labour. Tellingly, none has ever really considered paying users for the data they generate. The economics of data, too, put pressure on the price of data labour: why, for instance, should a firm pay a high price for an individual's data if it can infer them cheaply from another person's information?

A data economy in which those who produce a large part of the main input

are perennially underpaid is unlikely to be a healthy economy. Those with the greatest expertise, such as radiologists who can check the accuracy of an algorithm that recognises medical images, might hold back their knowledge and refuse to participate. Data workers with low pay and no say in the use of the information they generate will increasingly feel alienated, which could lower the quality of their work. And solving the problem through redistribution—as Gavin Newsom, California's Democratic governor, wants to do with a "digital dividend" to be levied from tech giants and disbursed

to the state’s citizens—would be a burden on the data economy and lead to trade conflicts. Such subsidies would be vulnerable to cuts as the political winds change.

All these complications explain why another proposed remedy keeps popping up: creating property rights on personal data to increase people’s bargaining power. Yet this in itself would not help much. If most people understandably ignore the complex privacy policies that come with online services, how can they be expected to shop around for the best price for their data? And property rights could actually make things worse.

Since most personal data are fundamentally a social construct to which more than one person has the right, individuals could engage in a race to the bottom. Each member of a family, say, could sell their genetic information and by doing so reveal much of their relatives' DNA.

Instead of giving citizens individual control over their data, they should hold it collectively, argues Mr Weyl. He and an activist organisation he helped found, RadicalxChange, want everyone to join what they call "data co-operatives". These would act much like trade unions in the conventional economy. They

would, among other things, negotiate rates for data work, ensure the quality of members' digital output, bill data firms that benefit from this output, and distribute the proceeds.

Like data trusts, robust data co-operatives will not emerge overnight. They need support from all involved. There are early signs that this may be forthcoming. Some Western countries may soon discuss a "Data Freedom Act", based on a draft by RadicalxChange, which would create a new regulated entity for that purpose. In a first for a tech-giant boss, Satya Nadella, the chief executive of

Microsoft, at the World Economic Forum in Davos in January called on the industry to show more respect for "data dignity"—meaning to give people more control over their data and a bigger share of the value these data create. The public, for its part, is getting ever more concerned about what happens with its data. Roughly eight in ten Americans, for instance, now think they have very little or no control over the data which companies collect about them.

Expect debates about such ideas as data co-operatives to become more heated as the data economy grows.

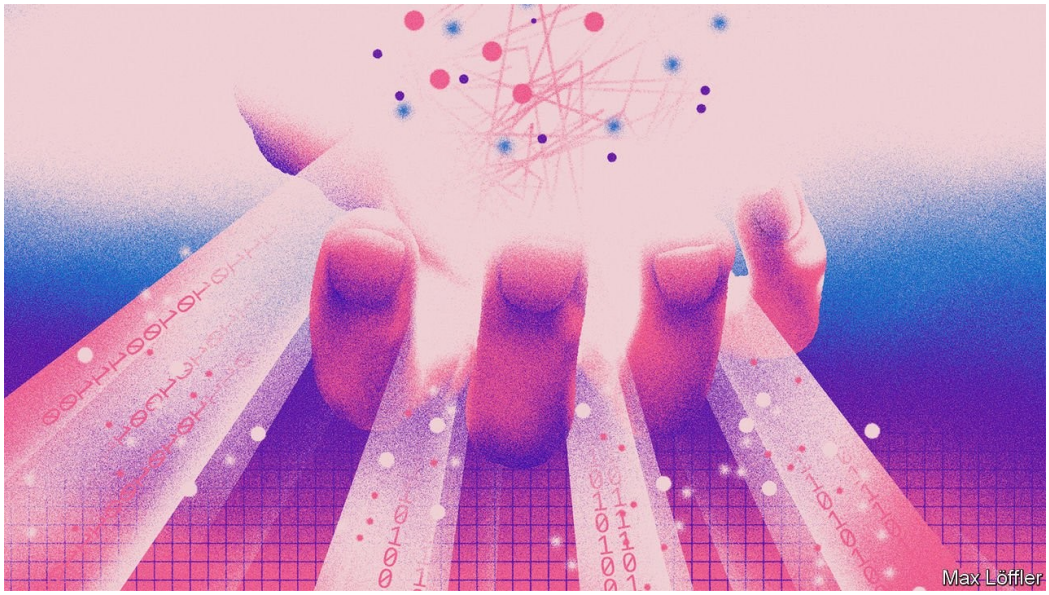
Encouragingly, as Mr Arthur points out, humanity has overcome a similar conundrum before. In the 1850s, the Industrial Revolution brought big increases in production, along with Dickensian social conditions. It took 100 years for societies to adapt; some never did. In the data economy, too, it will take a long time to build the appropriate mechanisms and institutions. No one yet worries that revolutions and wars will be fought over data, but there is no guarantee.

8. Are data more like oil or sunlight?

The question highlights the many different faces of data

The Economist

20200220



Source: https://www.economist.com/special-report/2020/02/20/are-data-more-like-oil-or-sunlight

PASSIONATE GRAMMARIANS have long quarrelled over whether data should be singular or plural (contrary to common usage, this newspaper is sticking with the latter, for now). A better question is why are data so singularly plural? That is, why do they have so many different faces?

For an answer, start with the many metaphors used to describe flows of data. Originally they were likened to oil, suggesting that data are the fuel of the future. More recently, the comparison has been with sunlight because soon, like solar rays, they will be everywhere and underlie everything. There is also

talk of data as infrastructure: they should be seen as a kind of digital twin of roads or railways, requiring public investment and new institutions to manage them.

The multiplication of metaphors reflects the malleable economics of data. First, they are “non-rivalrous”: since they are infinitely copyable, they can be used by many people without limiting the use by others. But they are also “excludable”: technologies like encryption can control who has access to them. Depending on where one sets the cryptographic slider, data can indeed be private goods like oil or public goods like sunlight—or

something in between, known as a “club good”.

This in turn means that there is not just one data economy, but three more or less distinct ones, each with its own ideology. And the big question is whether one will come to dominate, or whether the mirror world will be as much of a mixture as the real one.

If oil is still the most-used metaphor, it is because comparing data to the black stuff is easy. Like oil, data must be refined to be useful. In most cases they need to be “cleansed” and “tagged”, meaning stripped of inaccuracies and marked to identify what can be seen,

say, on a video. This has spawned a global industry employing hundreds of thousands of people, mostly in low-wage countries. Scale AI, a startup in San Francisco, employs 30,000 taggers around the world who review footage from self-driving cars and ensure the firm's software has correctly classified things like houses and pedestrians.

Before data can power AI services, they also need to be fed through algorithms, to teach them to recognise faces, steer self-driving cars and predict when jet engines need a check-up. And different data sets often need to be combined for statistical patterns to emerge. In the case

of jet engines, for instance, mixing usage and weather data helps forecast wear and tear.

The oil metaphor also rings true because some types of data and some of the insights extracted from them are already widely traded. Online advertising is perhaps the biggest marketplace for personal data: clicks are bought and sold based on a detailed digital profile of each viewer. It was worth $178bn globally in 2018, according to Strategy&, a consultancy. Data brokers, which can track thousands of data points for each individual, do brisk business with personal information, too.

They sell it to everyone from banks to telecoms carriers, generating annual revenue of more than $21bn, says Strategy&.

Offering insights from mining data can be very profitable, too. On Kaggle, a website owned by Google that hosts machine-learning contests, thousands of teams of data scientists compete against each other to see who can come up with the best algorithms to predict a building's energy consumption or to detect "deepfake" videos, with prizes sometimes exceeding $1m. That is also Facebook's and Google's way to make money. They hardly ever sell data, but

they do sell insights about who is the best target for advertising.

Yet data have failed to become “a new asset class”, as the World Economic Forum, a conference-organiser and think-tank, predicted in 2011. Most data never change hands, and attempts to make them more tradable have not taken off. To change this, especially in Europe, manufacturers are pushing to secure property rights for the data generated by their products. Others want consumers to own the data they create, so they can sell them and get a bigger cut from their information.

Again, economics gets in the way. Although data are often thought of as a commodity, corporate data sets, in particular, tend not to be fungible. Each is different in the way it was collected, and in its purpose and reliability. This makes it difficult for buyers and sellers to agree on a price: the value of each sort is hard to compare and changes over time. A further barrier to trading is that the value of a data set depends on who controls it. What might simply be data exhaust to one firm could be digital gold to another. “There is no true value of data,” says Diane Coyle of the University of Cambridge.

As for personal data, defining property rights is tricky, because much information cannot be attributed to one person. Who, for instance, owns the fact that a dating site has matched a couple? The couple themselves? Or the service? Complicating matters, data have plenty of externalities, both positive and negative, meaning that markets often fail. Why should a social network, say, buy the data of an individual if it can make quite accurate predictions about him by crunching data from other users?

Although data are unlikely ever to be traded as widely as oil, tech firms keep trying to make this easier. Amazon Web

Services (AWS), the cloud-computing arm of the e-commerce giant recently launched a marketplace that aims to make trading in data as easy as possible. It works a bit like an online store for smartphone apps: buyers subscribe to feeds, agree to licensing conditions, and AWS processes the payment.

As the oil metaphor is seen as increasingly problematic, the comparison to sunlight or similar resources, such as air and water, has risen in favour. Many people who prefer this metaphor ask if data do not really lend themselves to be turned into a tradable good, then why even try?

Would it not instead be better to ensure that data are used as much as possible? After all, this will maximise social wealth. In other words, nobody puts up curtains and tries to charge for sunlight.

This line of argument has already given birth to what is known as the “open-data” movement. Its champions push organisations and universities to give away their data so they can be widely used, for instance by startups. Today, most governments, national or otherwise, boast an open-data project, although the quality of the data made available varies greatly.

More recently, companies have started to publish their data, too. Several firms that work on self-driving cars have shared some of the information collected by their vehicles. “For researchers to ask the right questions, they need the right data,” according to Dragomir Anguelov, principal scientist at Waymo, a firm owned by Alphabet, Google’s parent, that is one of the companies that has done this. Others are working on technology to make such data-sharing easier: Microsoft and other software makers will soon start to implement what it calls the “open-data initiative”.

Some see such efforts as the beginning of an open-source movement for data, much like the approach that now rules large parts of the software industry. And Microsoft, in particular, is keen to see this happen. “We need to democratise AI and the data on which it relies,” writes Brad Smith, the firm’s president and chief legal officer in his recently published book, “Tools and Weapons”. Unsurprisingly, this position also smacks of self-interest: Microsoft does not make much money from data directly, but does from tools and services that handle data.

Like the oil comparison, however, the data-as-sunlight analogy breaks down: open data, too, can go only so far. For personal data, the main limitation is increasingly strict privacy laws, such as the EU's General Data Protection Regulation (GDPR), as well as the California Consumer Privacy Act (CCPA), which will start being enforced in July. For corporate data the checks are economic in nature: generating good data is expensive and they can reveal too much about a firm's products. "Companies will make very strategic decisions about what data sets they will make public and which ones they will

keep to themselves," explains Michael Chui of the McKinsey Global Institute, a consultancy think-tank.

Separating what can be safely shared from what should be closely guarded will be tricky, but technology should, in time, make such decisions easier. Something called "differential privacy", for instance, replaces one data set with another that includes different information, but has the same statistical patterns. "Homomorphic encryption" allows algorithms to crunch data without decrypting them. And blockchains, which are the special databases of the sort that underlie many

digital currencies, enable people and companies to manage in minute detail who is allowed to access what data and to track who has done so.

Slowly these technologies are being deployed. DECODE, an initiative financed until last year by the European Union, has used a combination of them to create tools that allow people to control the data they generate and collect about their environment, for instance, on noise levels and air quality. They are being tested in Amsterdam and Barcelona. Oasis Labs, another startup in San Francisco, has built something similar for health data. Its first service,

which will launch soon, will let users donate genetic information to research projects.

Such data-dividing technologies are also grist to the mill of those who liken data to infrastructure. You have to travel many digital roads—and combine many data sets and streams—to get to new insights, says Jeni Tennison, who heads the Open Data Institute, a research outfit based in Britain. Some will be private toll roads, others public multi-lane highways, but many need to be operated as shared digital resources managed in a “club” by users.

Yet technology alone will not be enough to create these “club goods”. They also need institutions that provide what Ms Tennison calls “data stewardship”. Data trusts, data co-operatives, personal data stores—all are different in detail, but the idea is essentially the same: they provide a governance structure to organise access to data in a way that takes into account the interests of those producing and using a particular sort of data.

It is early days, but such data clubs have started to pop up in many places. MIDATA is a Swiss co-operative that collects and manages members’ health-

care data. In Taiwan Audrey Tang, the digital minister, has created an ongoing “Presidential Hackathon” to set up “data collaboratives”, including several for environmental data. In Finland, Sitra, a policy outfit, has launched a similar competition to help get “fair data exchanges” off the ground.

New thing on the old continent

Most projects are still small and live on the public dime, which raises doubts about whether they will ever be a big part of the data economy. But whether they are successful or not is a question of political will, says Francesca Bria, the founder of the DECODE project.

Cities in particular, she argues, need to create alternatives to the big online platforms, which treat data they collect as their own. A former chief technology officer of Barcelona, she turned the city into a model of what is possible, which is now copied elsewhere in Europe. Not only can Barcelona's citizens control the data the city holds on them, but its suppliers must add the information they gather while delivering services to the municipal data commons.

Given their respective limitations, none of the three sorts of data economies will dominate, but they are likely to have strongholds. In America data are treated

like oil: whoever extracts them owns them. China—although it, too, has data-hungry online platforms of its own, including Alibaba and Tencent—is an extreme example of a place where data are public goods. They are ultimately controlled by the government, which is pushing firms to pool certain types, such as health data. In Europe, many regulators have come to see data as infrastructure. The new European Commission in Brussels has big plans to support the creation of data trusts.

This sounds as if the EU is about to condemn itself to remaining a tech laggard. But this need not be the case. A

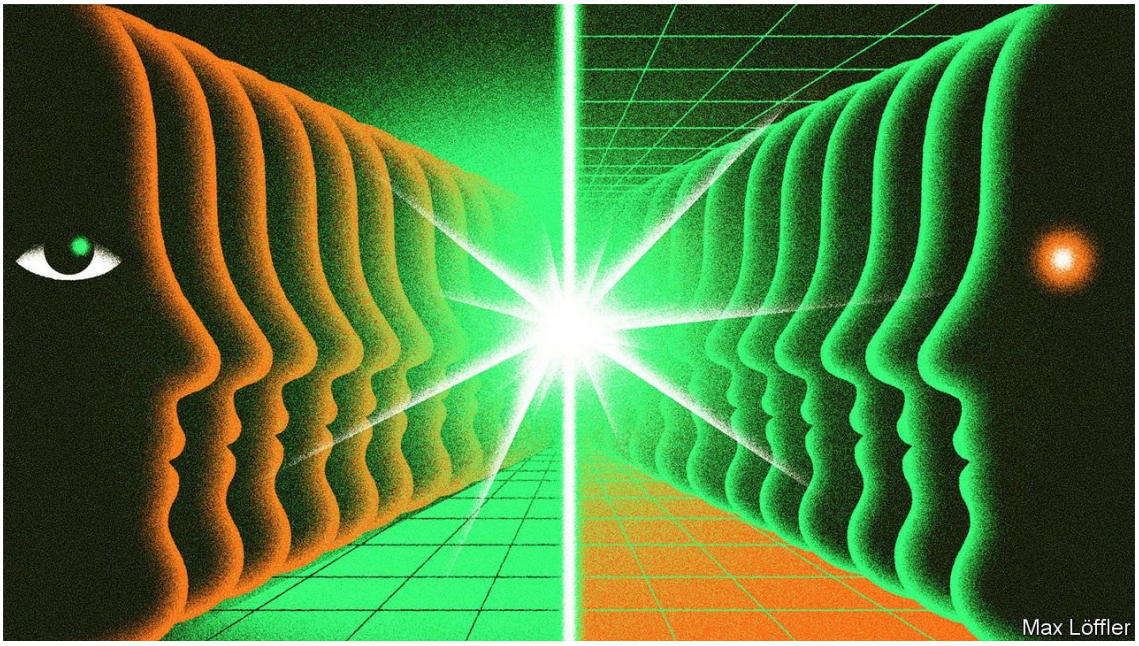
“fair data-economy”—one that takes into account the interests of citizens and consumers, who will generate much of the fuel of the future—may prove to be quite competitive, says Luukas Ilves, the co-author of a report for Sitra in Finland. If people, as well as firms, can trust the continent’s data infrastructure, they will be willing to share more and better data, which means better services for everyone. If such a “virtuous cycle” were to take off, it would be quite a reversal of the old world’s fortunes

9. A deluge of data is giving rise to a new economy

Ludwig Siegele asks how it will work

The Economist

20200220



Source:

https://www.economist.com/special-report/2020/02/20/a-deluge-of-data-is-giving-rise-to-a-new-economy

AN ARMY OF doppelgangers is invading the world. Digital copies of aircraft engines, wind turbines and other heavy equipment came first. Now the electronic ghosts of smaller and larger things are joining them in the virtual realm, from toothbrushes and traffic lights to entire shops and factories. Even humans have begun developing these alter egos. In America the National Football League is planning to design an electronic avatar for every player.

These “digital twins”, as geeks term them, are far more than replicas of the original. Think of them more as

shadows that are, thanks to a multitude of sensors and wireless connectivity, intimately linked to their physical selves, and every day producing oceans of data. If something happens in the real world, it is rapidly reflected in this shadow realm. Some digital twins already come with the laws of nature programmed in. They double as a database of everything that has ever happened to the original. This makes it possible to look into their future. Sports coaches, for instance, will be able to run simulations, predict when an athlete might get injured and adjust training routines to avoid problems.

Digital twins are just one part of a vast shift in the world's economy. They populate what David Gelernter of Yale University long ago forecast as "mirror worlds": a new dimension of human life based on and fuelled by data. Year by year, ever more parts of the physical realm are coming to be represented and simulated in the virtual world—an inversion of Plato's theory that real-world objects are just imperfect copies of their true being in the spiritual realm. The emergence of these mirror worlds will bring about a distinct economy. This development will require new markets, institutions, infrastructure,

businesses and even geopolitical arrangements. It is the promises and pitfalls of the new “data economy” which will be the focus of this special report.

Mirror worlds are not mere mathematical representations of real ones. They also give new meaning to the adage that knowledge is power. Increasingly, digital copies are taking on lives of their own and acting on the physical world. They can be used to optimise everything, from the acoustics of a headset to an entire national railway network. They will enable all sorts of artificial-intelligence (AI)

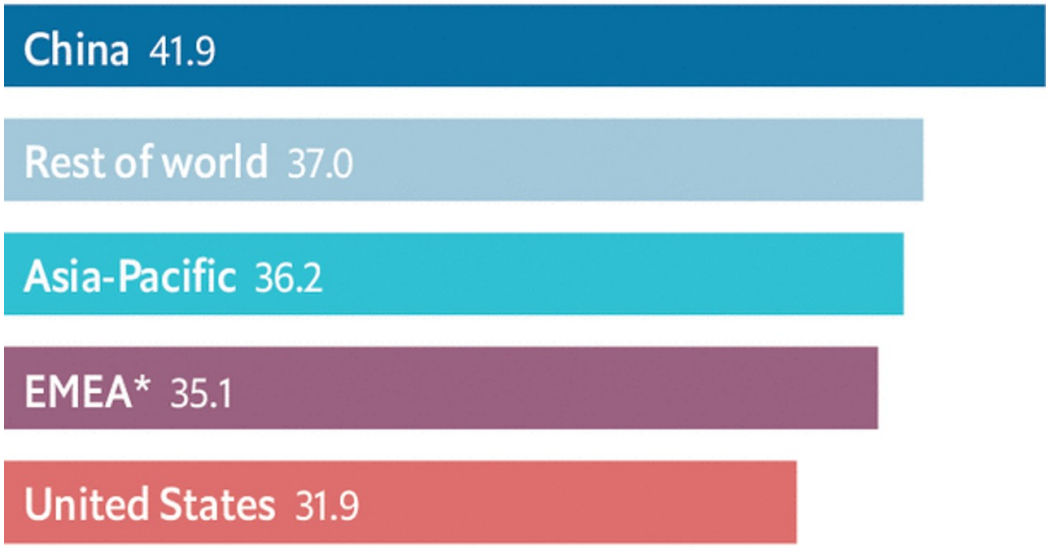
algorithms to recognise objects and faces, understand speech and even distinguish smells. And they make possible new business models: why buy heavy equipment if its wear and tear can be measured in detail and it can thus be rented by the minute?

Deluged

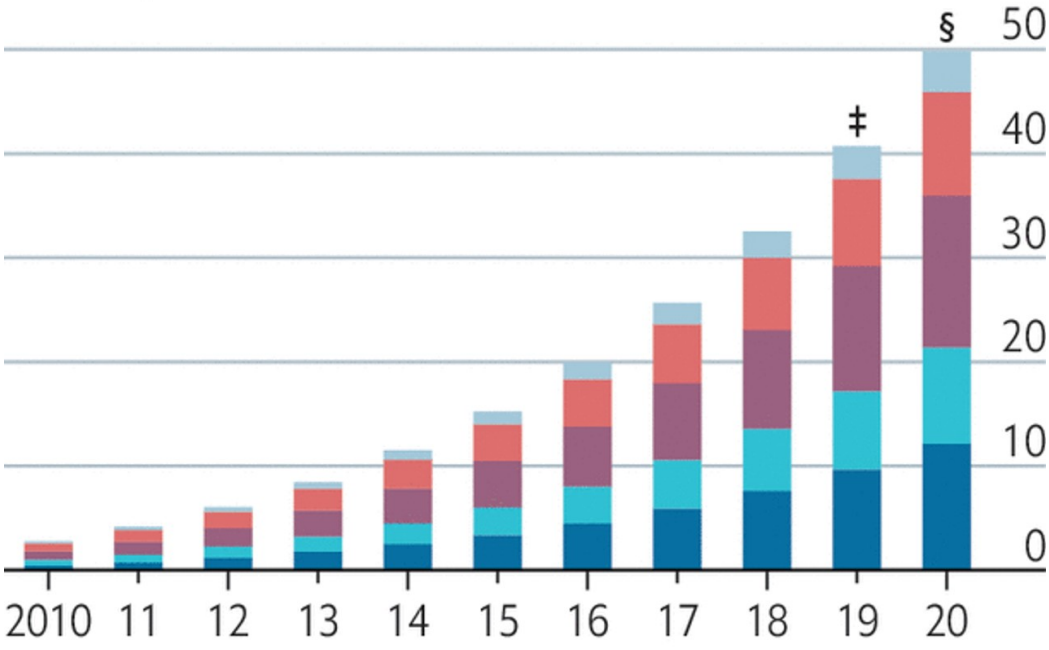
Data generated, worldwide

Average annual increase

2010-18, %



Zettabytes†



*Europe, Middle East and Africa

Source: IDC, Seagate

†1ZB=1 trillion GB ‡Estimate §Forecast

The Economist

A good place to start analysing any economy is by measuring it. A robust methodology has yet to be developed, but the data economy is already large. Statistics Canada, a government agency, last year tried to estimate the value of the country's data (its stock plus related software and intellectual property in the field). The result was between C$157bn and C$218bn ($118bn and $164bn). If that number is close—a big "if"—the value of all the data in America, whose GDP is 12 times that of Canada, could amount to $1.4trn-2trn, which would be nearly 5% of America's stock of private physical capital.

If the amount of data generated around the world is any guide, this new economy is growing fast. The first human genome (three gigabytes of data, which nearly fills a DVD) was sequenced 17 years ago; in April, 23andMe, a firm which offers genetic testing, claimed more than 10m customers. The latest autonomous vehicles produce up to 30 terabytes for every eight hours of driving (or some 6,400 DVDs). IDC, a market-research firm, estimates the world will generate about 90 zettabytes (19trn DVDs) this year and next (see chart), more than all

data produced since the advent of computers.

Yet even more striking than the rapid growth of the data economy are the tensions and trade-offs it produces. Take its economics. In some ways, data are a natural resource, much like oil, which can be owned and traded (this newspaper called data the “world’s most valuable resource” in 2017). But data also have characteristics of a public good, which ought to be used as widely as possible to maximise wealth creation. New institutions must be created to reflect this tension, as was the case for intellectual property.

The infrastructure of the data economy, too, is torn between two poles. Currently, it mainly consists of huge data centres packed with servers where data are stored and crunched. Yet such centralisation has drawbacks, not least because it consumes huge amounts of energy and creates privacy risks. A decentralising counter-movement is already under way: more data are processed at the “edge”, closer to where they are collected.

Businesses are also facing a digital reversal. Many firms want to use data to infuse their corporate applications with AI. They have built central repositories

such as “data lakes”, which hold all kinds of digital information. Such systems are of limited use, however, if a firm and its employees lack the required skills, refuse to believe the data or even to share them internally.

Finally, the geopolitics of data will not be simple, either. Online giants in particular have assumed that the data economy will be a global affair, with the digital stuff flowing to where processing is best done for technical and cost reasons. Yet governments are increasingly asserting their “digital sovereignty”, demanding that data not leave their country of origin.

This special report will tackle these topics in turn. It will conclude by discussing what is perhaps the biggest conundrum of the mirror world: the risk is that the wealth it creates will be even more unequally distributed than in its terrestrial twin.

10. Techno-tyrannie : Comment l’Etat sécuritaire étatsunien utilise la crise du coronavirus pour concrétiser une vision digne d’Orwell

Par Whitney Webb, 20200520

Source utilisée: https://lesakerfrancophone.fr/techno-tyrannie-comment-letat-securitaire-etatsunien-utilise-la-crise-du-coronavirus-pour-concretiser-une-vision-digne-dorwell traduit par Wayan le 20200506 er relu par Marcel pour le Saker francophone.

Source primaire : https://www.thelastamericanvagabond.com/top-news/techno-tyranny-how-us-national-security-state-using-coronavirus-fulfill-orwellian-vision/

L’année dernière, une commission gouvernementale demandait aux États-Unis d’adopter un système de surveillance de masse piloté par l’intelligence artificielle allant bien au-delà de celui utilisé par tout autre pays, afin de garantir l’hégémonie étasunienne en ce domaine. Aujourd’hui, nombre d’obstacles qui étaient cités comme empêchant sa mise en œuvre sont rapidement franchis sous couvert de lutte contre le coronavirus.

L’année dernière, un organe du gouvernement américain chargé d’examiner comment l’intelligence artificielle peut « répondre aux besoins

de la sécurité nationale et de la défense des États-Unis » a examiné en détail les changements « structurels » que l'économie et la société américaines devaient subir afin de s'assurer un avantage technologique sur la Chine, selon un document récent acquis grâce à une demande de type FOIA [Freedom of Information Act]. Ce document suggère que les États-Unis devraient suivre l'exemple de la Chine et même la surpasser dans de nombreux aspects liés aux technologies basées sur l'IA, en particulier leur utilisation de la surveillance de masse. Cette perspective se heurte clairement à la rhétorique

publique des hauts fonctionnaires et des politiciens américains sur la Chine, qui ont qualifié les investissements technologiques du gouvernement chinois et l'exportation de ses systèmes de surveillance et d'autres technologies de « menace » majeure pour le « mode de vie » des Américains.

Par contre, de nombreuses mesures pour la concrétisation d'un tel programme aux États-Unis, telles que présentées dans ce document, sont actuellement promues et mises en œuvre dans le cadre de la réponse du gouvernement à la crise actuelle du coronavirus (Covid-19). Ceci est probablement dû au fait

que de nombreux membres de ce même organisme ont des chevauchements considérables avec les groupes de travail qui guident actuellement les plans du gouvernement pour « rouvrir l'économie » et utiliser la technologie pour répondre à la crise actuelle.

Ce document, obtenu par l'Electronic Privacy Information Center (EPIC), a été rédigé par une organisation gouvernementale américaine peu connue appelée National Security Commission on Artificial Intelligence (NSCAI). Cette organisation a été créée par le National Defense Authorization Act (NDAA) de 2018 et son objectif

officiel est « d’examiner les méthodes et les moyens nécessaires pour faire progresser le développement de l’intelligence artificielle (IA), l’apprentissage machine et les technologies associées afin de répondre de manière exhaustive aux besoins de sécurité et de défense nationale des États-Unis ».

La NSCAI est donc un élément clé de la réponse du gouvernement à ce que l’on appelle souvent la « quatrième révolution industrielle » à venir, qui a été décrite comme « une révolution caractérisée par un développement technologique ininterrompu dans des

domaines comme l’intelligence artificielle (IA), les grandes base de données, les réseaux de télécommunications de cinquième génération (5G), la nanotechnologie et la biotechnologie, la robotique, l’Internet des objets (IoT) et l’informatique quantique ».

Cependant, son objectif principal est de s’assurer que « les États-Unis… maintiennent un avantage technologique dans les domaines de l’intelligence artificielle, de l’apprentissage machine et autres technologies associées liées à la sécurité et à la défense nationales ».

Le vice-président de la NSCAI, Robert

Work – ancien secrétaire adjoint à la défense et chercheur principal au Centre pour une nouvelle sécurité américaine (CNAS), a décrit l'objectif de la commission comme étant de déterminer « comment l'appareil de sécurité nationale des États-Unis devrait aborder l'intelligence artificielle, en se concentrant notamment sur la manière dont le gouvernement peut travailler avec l'industrie pour concurrencer le concept chinois de 'fusion civil-militaire' ».

Le récent document de la NSCAI fut publié en mai 2019 et intitulé « Chinese Tech Landscape Overview » [vue

d’ensemble du paysage technologique chinois]. Tout au long de la présentation, la NSCAI promeut une refonte de l’économie et du mode de vie des États-Unis comme étant nécessaire pour permettre de s’assurer qu’ils détiennent un avantage technologique considérable sur la Chine, car la perte de cet avantage est actuellement considérée comme un problème majeur de « sécurité nationale » par l’appareil de sécurité nationale américain. Cette préoccupation concernant le maintien d’un avantage technologique se retrouve dans plusieurs autres documents militaires et rapports de groupes de

réflexion américains qui avertissent que l’avantage technologique des États-Unis s’effrite rapidement.

Le gouvernement américain et les médias grand public blâment souvent le prétendu espionnage chinois ou les partenariats plus explicites du gouvernement chinois avec des entreprises technologiques privées pour étayer leur affirmation selon laquelle les États-Unis perdent cet avantage sur la Chine. Par exemple, Chris Darby, l’actuel PDG de la société In-Q-Tel de la CIA, qui fait également partie du NSCAI, a déclaré l’année dernière à CBS News que la Chine est le principal

concurrent des États-Unis en termes de technologie et que les lois américaines sur la protection de la vie privée entravaient la capacité des États-Unis à contrer la Chine à cet égard :

> *"Les datas sont le nouveau pétrole. Et la Chine est tout simplement inondée de données. Elle n'a pas les mêmes contraintes que nous en ce qui concerne la collecte et l'utilisation des données, en raison de la différence de protection de la vie privée entre nos pays. Le fait qu'ils possèdent le plus grand ensemble de données étiquetées au monde va être une force énorme pour eux."*

Dans un autre exemple, Michael Dempsey – ancien directeur intérimaire du renseignement national et

actuellement boursier du Council on Foreign Relations financé par le gouvernement – expliquait dans The Hill que :

> Il est clair, cependant, que la Chine est déterminée à dépasser notre avantage technologique, et qu'elle engage des centaines de milliards de dollars dans cet effort. En particulier, la Chine est déterminée à être un leader mondial dans des domaines tels que l'intelligence artificielle, le calcul haute performance et la biologie synthétique. Ce sont ces industries qui façonneront la vie sur la planète et l'équilibre militaire du

pouvoir pour les prochaines décennies.

En fait, l’appareil de sécurité nationale des États-Unis est tellement préoccupé par la perte de son avantage technologique sur la Chine que le Pentagone a récemment décidé de s’associer directement à la communauté du renseignement américaine afin de « devancer les avancées chinoises en matière d’intelligence artificielle ». Cette union a abouti à la création du Centre conjoint pour l’intelligence artificiel (JAIC), qui relie « les efforts des militaires avec ceux de la communauté du renseignement, leur

permettant de combiner leurs efforts pour faire avancer les initiatives gouvernementales en matière d'IA ». Ce centre assure également la coordination avec d'autres organismes gouvernementaux, l'industrie, les universitaires et les alliés des États-Unis. Robert Work, qui est devenu par la suite vice-président du NSCAI, déclarait à l'époque que la création du JAIC était « une première étape bienvenue en réponse aux plans chinois, et dans une moindre mesure, russes, visant à dominer ces technologies ».

Des préoccupations similaires concernant la « perte » de l'avantage

technologique au profit de la Chine ont également été exprimées par le président de la NSCAI, Eric Schmidt, l'ancien directeur d'Alphabet – la société mère de Google, qui affirmait en février dans le New York Times que la Silicon Valley pourrait bientôt perdre « la guerre technologique » au profit de la Chine si le gouvernement américain ne prenait pas de mesures. Ainsi, les trois principaux groupes représentés au sein de la NSCAI – la communauté du renseignement, le Pentagone et la Silicon Valley – considèrent tous les progrès de la Chine en matière d'IA comme une menace majeure pour la

sécurité nationale (et dans le cas de la Silicon Valley, une menace pour leurs résultats et leurs parts de marché) à laquelle il faut s'attaquer rapidement.

Cibler l'avantage chinois de « *l'adoption* »

Dans sa présentation de mai 2019 intitulée « Chinese Tech Landscape Overview », la NSCAI explique que si les États-Unis sont toujours en tête au stade de la « création » d'IA et des technologies connexes, ils sont en retard sur la Chine au stade de l'« adoption » en raison de « facteurs structurels ». Elle affirme que la « création », suivie de l'« adoption » et de l'« itération »

sont les trois phases du « cycle de vie des nouvelles technologies » et affirme que si la phase d'« adoption » n'est pas rapidement dominée, la Chine pourra « dépasser » les États-Unis et dominer l'IA dans un avenir prévisible.

La présentation soutient également que pour dépasser les concurrents sur les marchés émergents ce qui est nécessaire n'est pas « l'intelligence individuelle » mais plutôt des « conditions structurelles spécifiques qui existent au sein de certains marchés ». Il cite plusieurs études de cas où la Chine est considérée comme dépassant les États-Unis en raison de différences majeures

dans ces « facteurs structurels ». Ainsi, l'insinuation du document (bien que cela ne soit pas directement énoncé) est que les États-Unis doivent modifier les « facteurs structurels » qui sont actuellement responsables de leur retard par rapport à la Chine dans la phase d'« adoption » des technologies basées sur l'IA.

Parmi les « facteurs structurels » problématiques soulignés dans cette présentation, les « systèmes culturels » qui sont courants aux États-Unis et beaucoup moins en Chine. Le document de la NSCAI indique que des exemples de « systèmes culturels » sont un

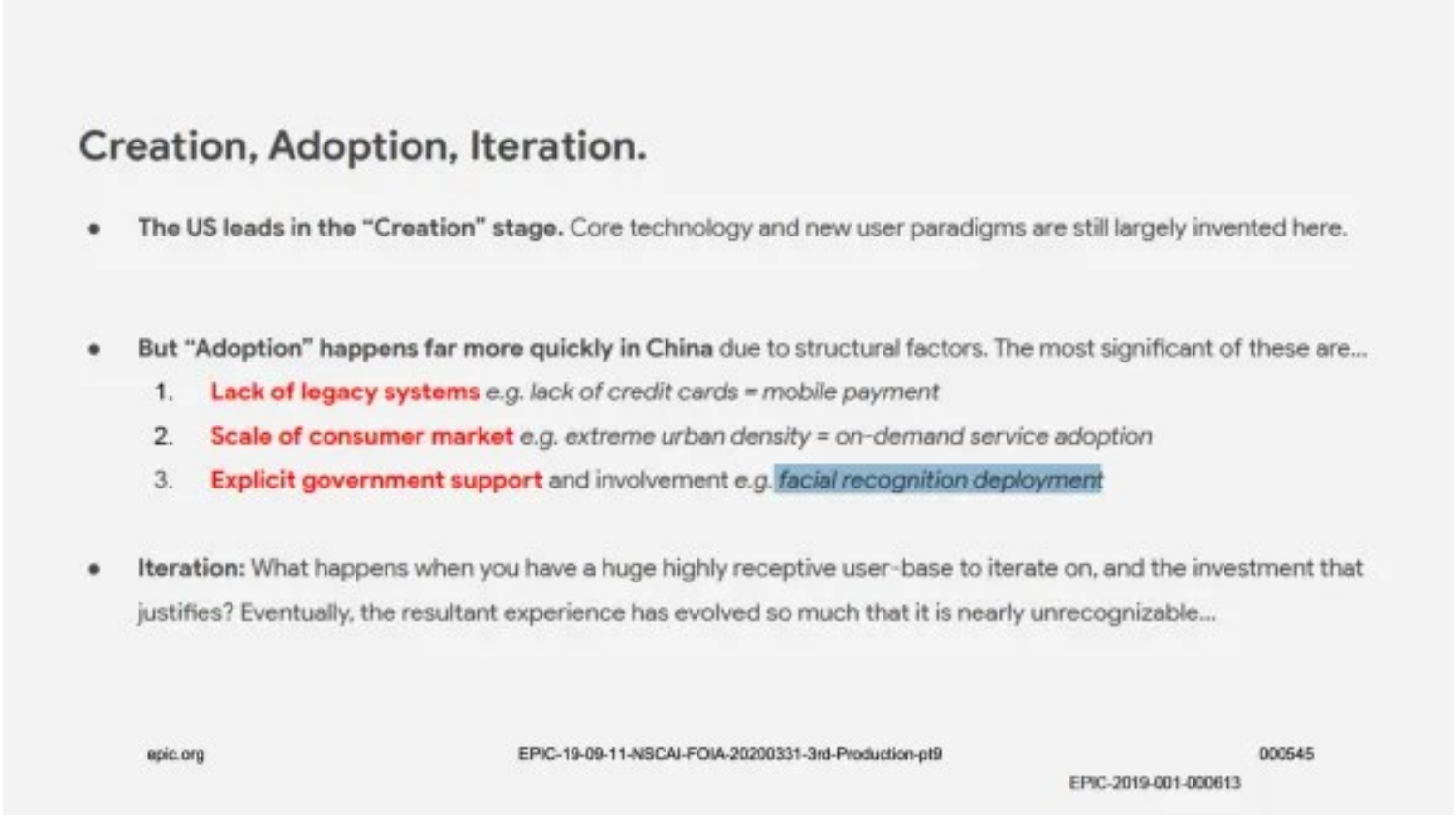
système financier qui utilise encore les paiements en espèces et par carte, la possession d'une voiture individuelle et même le fait de recevoir des soins médicaux d'un médecin humain.

Il indique que si ces « systèmes culturels » aux États-Unis sont « assez bons », trop de systèmes « assez bons » « entravent l'adoption de nouvelles

choses », en particulier les systèmes basés sur l'IA.

Un autre facteur structurel considéré par le NSCAI comme un obstacle à la capacité des États-Unis à maintenir un avantage technologique sur la Chine est « l'échelle du marché de consommation », en faisant valoir qu'une « extrême densité urbaine = l'adoption de services à la demande ». En d'autres termes, l'urbanisation extrême a pour conséquence qu'un plus grand nombre de personnes utilisent des services « à la demande » en ligne ou sur le téléphone portable, allant du covoiturage aux

achats en ligne. Elle cite également l’utilisation de la surveillance de masse sur l’« énorme base de population » chinoise, qui est un exemple de l’avantage de l’« échelle du marché de consommation » de la Chine permettant à celle-ci de « faire un bond en avant » dans les domaines des technologies connexes, comme la reconnaissance faciale.



Creation, Adoption, Iteration.

- **The US leads in the "Creation" stage.** Core technology and new user paradigms are still largely invented here.

- **But "Adoption" happens far more quickly in China** due to structural factors. The most significant of these are...
  1. **Lack of legacy systems** *e.g. lack of credit cards = mobile payment*
  2. **Scale of consumer market** *e.g. extreme urban density = on-demand service adoption*
  3. **Explicit government support** and involvement *e.g. facial recognition deployment*

- **Iteration:** What happens when you have a huge highly receptive user-base to iterate on, and the investment that justifies? Eventually, the resultant experience has evolved so much that it is nearly unrecognizable...

epic.org EPIC-19-09-11-NSCAI-FOIA-20200331-3rd-Production-pt9 000545

EPIC-2019-001-000613

Outre les prétendues lacunes des « systèmes culturels » des États-Unis et le manque de « densité urbaine extrême », la NSCAI appelle également à un « soutien et une participation plus explicite du gouvernement » comme moyen d'accélérer l'adoption de ces systèmes aux États-Unis. Cela inclut le prêt par le gouvernement de ses stocks

de données sur les civils pour entraîner l'IA [machine learning, NdSF], en citant spécifiquement les bases de données de reconnaissance faciale, et en exigeant que les villes soient « réarchitecturées autour des AV [véhicules autonomes] », entre autres. D'autres exemples sont donnés, comme l'investissement par le gouvernement d'importantes sommes d'argent dans des start-ups d'IA et l'ajout de mastodontes technologiques à un groupe de travail national public-privé sur l'IA, qui se concentrerait sur la mise en œuvre de villes intelligentes (entre autres).

En ce qui concerne ce dernier point, le document indique que « ce niveau de coopération public-privé » en Chine est « largement adopté » par les parties concernées, ce qui « contraste fortement avec la controverse autour de la Silicon Valley vendant au gouvernement américain ». Du point de vue de la NSCAI, les exemples d'une telle controverse incluent probablement les employés de Google qui ont demandé la fin du « Project Maven » du Pentagone, qui utilisait le logiciel d'intelligence artificielle de Google pour analyser les images capturées par les drones. Google a finalement choisi de ne pas renouveler

le contrat à la suite de cette controverse, même si les dirigeants de Google considéraient le projet comme une « occasion en or » de collaborer plus étroitement avec l'armée et les services de renseignement.

Le document définit également un autre aspect de l'aide gouvernementale comme le « démantèlement des barrières réglementaires ». Ce terme est utilisé dans le document spécifiquement en ce qui concerne les lois américaines sur la vie privée, malgré le fait que l'État américain de sécurité nationale viole depuis longtemps ces lois en toute

impunité. Cependant, le document semble suggérer que les lois sur la vie privée aux États-Unis devraient être modifiées afin que ce que le gouvernement américain fait « en secret » avec les données des citoyens privés puisse être fait de manière plus ouverte et plus étendue. Le document de la NSCAI aborde également la question de la suppression des « barrières réglementaires » afin d'accélérer l'adoption des voitures à conduite autonome, même si cette technologie a provoqué plusieurs accidents de voiture horribles et mortels et présente d'autres problèmes de sécurité.

Il y est également question de la façon dont l'« avantage chinois pour l'adoption lui permettra de dépasser les États-Unis » dans plusieurs nouveaux domaines, notamment le « diagnostic médical de l'IA » et les « villes intelligentes ». Il affirme ensuite que « l'avenir se décidera à l'intersection de l'entreprise privée et des dirigeants politiques entre la Chine et les États-Unis ». Si cette coordination sur le marché mondial de l'IA n'a pas lieu, le document avertit que « nous [les États-Unis] risquons d'être exclus des discussions où les normes relatives à

l’IA seront fixées pour le reste de notre vie ».

La présentation s’attarde également sur le fait que « le principal champ de bataille [en matière de technologie] n’est pas le marché domestique chinois et américain », mais ce qu’elle appelle les marchés NBU (next billion users, [le prochain milliard d’utilisateurs]), où elle affirme que « les acteurs chinois vont défier la Silicon Valley de manière agressive ». Afin de les défier avec plus de succès, la présentation affirme que « tout comme nous [considérons] le marché des adolescents comme un signe

avant-coureur des nouvelles tendances, nous devrions observer la Chine ».

Le document exprime également des inquiétudes quant au fait que la Chine exporte l'IA de manière plus étendue et plus intensive que les États-Unis, affirmant que la Chine « traverse déjà les frontières » en aidant à construire des bases de données de visages au Zimbabwe et en vendant des systèmes de reconnaissance d'images et des villes intelligentes à la Malaisie. Si elle est autorisée à devenir « le leader incontestable de l'IA », elle pourrait « finir par écrire une grande partie des

normes internationales relatives au déploiement de l'IA » et « élargir sa sphère d'influence au sein d'une communauté internationale qui se tourne de plus en plus vers l'autoritarisme pragmatique de la Chine et de Singapour comme alternative à la démocratie libérale occidentale».

Qu'est ce qui va remplacer les « *systèmes culturels* » des États-Unis ?

Étant donné que le document indique très clairement que les « systèmes culturels » aux États-Unis entravent leur capacité à empêcher la Chine de les

dépasser en matière d'IA et de dominer ce domaine dans un avenir prévisible, il est également important d'examiner ce que le document suggère pour remplacer ces « systèmes culturels » aux États-Unis.

Comme mentionné précédemment, un des « systèmes culturels » cités au début de la présentation est le moyen de paiement pour la plupart des Américains, à savoir l'argent liquide et les cartes de crédit/débit. La présentation affirme que, contrairement à ces « systèmes culturels », le meilleur et le plus avancé des systèmes est le

portefeuille numérique hébergé sur les smartphones.

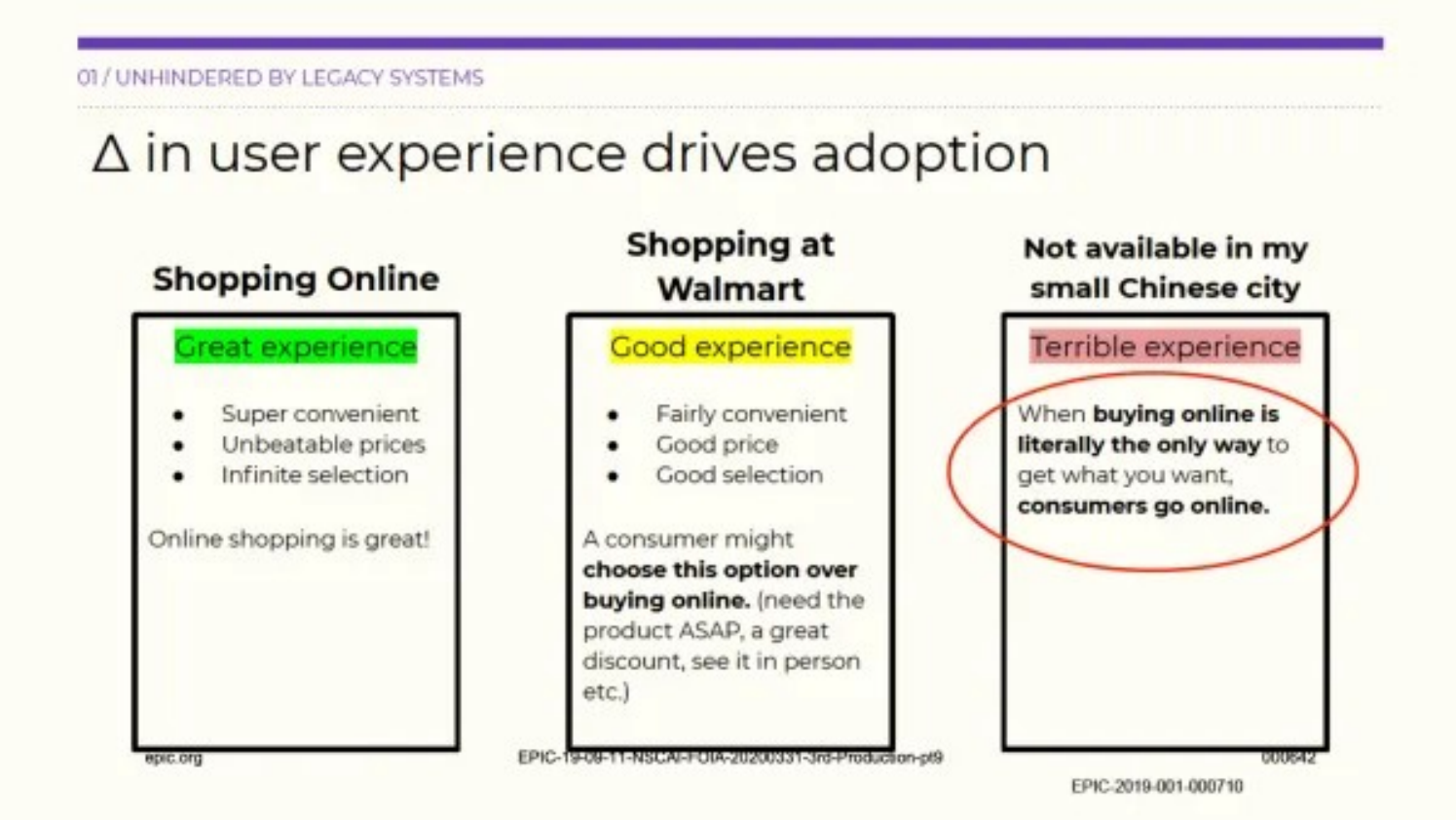
Il est noté en particulier que le principal fournisseur de portefeuilles mobiles en Inde, PayTM, est détenu en majorité par des sociétés chinoises. Un article cité affirme qu'« une grande rupture a eu lieu [en 2016] lorsque l'Inde a annulé 86% des devises en circulation dans un effort pour réduire la corruption et faire entrer plus de gens dans le filet fiscal en les forçant à utiliser moins d'argent liquide ». A l'époque, les affirmations selon lesquelles la « réforme monétaire » de l'Inde de 2016 servirait de tremplin

vers une société sans numéraire ont été rejetées par certains comme une « théorie du complot ». Cependant, l'année dernière, un comité réuni par la banque centrale indienne (et dirigé par un oligarque indien de la technologie qui a également créé l'énorme base de données biométriques civiles de l'Inde) a accouché du programme « Cashless India » du gouvernement indien.

Concernant la « réforme monétaire » de l'Inde de 2016, le document de la NSCAI affirme ensuite que « cela serait impensable en Occident. Et sans surprise, lorsque 86% des espèces ont

été annulées et que personne n'avait de carte de crédit, les « portefeuilles électroniques » en Inde ont explosé, posant les bases d'un écosystème de paiements bien plus avancé en Inde qu'aux États-Unis. » Cependant, cela est devenu de moins en moins impensable à la lumière de la crise actuelle du coronavirus, qui a vu des efforts pour réduire le montant des liquidités utilisées parce que les billets de banque en papier peuvent transporter le virus ainsi que des efforts pour introduire un « dollar numérique » soutenu par la Réserve fédérale.

En outre, le document de la NSCAI de mai dernier appelle à la fin des achats en boutique et encourage l’évolution vers un système où tous les achats sont effectués en ligne. Il affirme que « les entreprises américaines ont beaucoup à gagner en adoptant les idées des entreprises chinoises » en se tournant vers des options d’achat exclusivement en ligne. Il affirme que seul le shopping en ligne offre une « expérience formidable » et ajoute également que « lorsque l’achat en ligne est littéralement le seul moyen d’obtenir ce que vous voulez, alors les consommateurs achètent en ligne ».



La NSCAI cherche également à réviser un autre « système culturel », celui de la propriété automobile, car il encourage les véhicules autonomes, ou sans chauffeurs, et affirme en outre que la « propriété d'une flotte de voitures > propriété d'une seule voiture ». Elle souligne en particulier la nécessité d'un « réseau centralisé de covoiturage » qui,

selon elle, « est nécessaire pour coordonner les voitures afin d'atteindre des taux d'utilisation proches de 100 % ». Toutefois, elle met en garde contre les réseaux de covoiturage qui « ont besoin d'un opérateur humain associé à chaque véhicule » et affirme également que « la possession d'une flotte de voitures a plus de sens » que la possession d'une voiture individuelle. Elle demande aussi spécifiquement que ces flottes de voitures ne soient pas seulement composées de voitures à conduite autonome, mais aussi de voitures électriques et cite des rapports selon lesquels la Chine « a les objectifs les

plus agressifs au monde en matière de véhicules électriques… et cherche à prendre la tête d'une industrie émergente ».

Le document affirme que la Chine est aujourd'hui en tête dans le domaine du covoiturage, même si le covoiturage a d'abord été introduit aux États-Unis. Il affirme une fois de plus que le « système culturel » américain de possession de voitures individuelles et l'absence de « densité urbaine extrême » sont responsables de l'avance chinoise en ce domaine. Il prédit également que la Chine « parviendra à une adoption

massive de véhicules autonomes avant les États-Unis », en grande partie parce que « l'absence de possession massive de voitures [en Chine] conduit à une plus grande réceptivité des consommateurs aux AV [véhicules autonomes] ». Il note ensuite que « l'adoption rapide et en masse conduit à un cycle vertueux qui permet à la technologie chinoise de conduite sans chauffeur d'accélérer et dépasser ses homologues occidentaux ».

En plus de sa vision d'un futur système financier et d'un futur système de transport autonome, la NSCAI a une

vision dystopique similaire pour la surveillance. Le document appelle la surveillance de masse « un des premiers et meilleurs clients pour l'IA » et « une application tueuse pour l'apprentissage profond [deep learning, NdSF] ». Il indique également que « le fait d'avoir des rues inondées de caméras est une bonne infrastructure ».

Il examine ensuite la façon dont « une génération entière de licornes de l'IA » perçoivent la majeure partie de leurs premiers revenus des contrats de sécurité du gouvernement et fait l'éloge de l'utilisation de l'IA pour faciliter les

activités de police. Par exemple, il salue les rapports selon lesquels « la police prononce des condamnations sur la base d'appels téléphoniques contrôlés par la technologie de reconnaissance vocale d'iFlyTek » et que « les services de police utilisent la technologie de reconnaissance faciale [AI] pour aider à tout, de l'arrestation des contrevenants au code de la route à la résolution des affaires de meurtre ».

En ce qui concerne plus particulièrement la technologie de reconnaissance faciale, le document de la NSCAI affirme que la Chine a « fait

un bond en avant » par rapport aux États-Unis en matière de reconnaissance faciale, même si « les percées dans l'utilisation de l'apprentissage automatique pour la reconnaissance d'images ont initialement eu lieu aux États-Unis ». Elle affirme que l'avantage de la Chine dans ce cas est que le gouvernement a mis en place une surveillance de masse (« suppression des barrières réglementaires »), d'énormes réserves de données fournies par le gouvernement (« soutien explicite du gouvernement ») combinées à des bases de données du secteur privé sur une énorme base de population («

échelle du marché de consommation »). Selon le NSCAI, la Chine est donc sur le point de dépasser les États-Unis en matière de reconnaissance faciale et d'image ainsi que de biométrie.

Le document souligne également une autre différence flagrante entre les États-Unis et leur rival, en affirmant : « Dans la presse et la politique américaine et européenne, l'IA est dépeint comme un objet de crainte qui érode la vie privée et vole des emplois. À l'inverse, la Chine le considère à la fois comme un outil pour résoudre les grands défis macroéconomiques afin de pérenniser

son miracle économique, et comme une opportunité de prendre le leadership technologique sur la scène mondiale ».

Le document de la NSCAI aborde également le domaine des soins de santé, appelant à la mise en place d'un système qui semble devenir réalité grâce à la crise actuelle du coronavirus. En parlant de l'utilisation de l'IA dans les soins de santé (près d'un an avant le début de la crise actuelle), il affirme que « la Chine pourrait être le leader mondial dans ce secteur » et « cela pourrait l'amener à exporter sa technologie et à établir des normes

internationales ». L’une des raisons de cette situation est également que la Chine a « bien trop peu de médecins pour la population » et la NSCAI considère que le fait d’avoir suffisamment de médecins pour les visites en personne est un « système culturel ». Le document cite également les mesures réglementaires américaines telles que « la conformité à la HIPPA [Health Insurance Portability and Accountability Act] et l’approbation de la FDA [Food and Drug administration] » comme des obstacles qui ne contraignent pas les autorités chinoises.

Plus troublant encore, il affirme que « l'impact potentiel des données fournies par le gouvernement est encore plus important dans le domaine de la biologie et des soins de santé », et dit qu'il est probable que « le gouvernement chinois [va] exiger que chaque citoyen ait son ADN séquencé et stocké dans les bases de données gouvernementales, ce qui est presque impossible à imaginer dans des endroits aussi soucieux de la vie privée que les États-Unis et l'Europe ». Il poursuit en disant que « la bureaucratie chinoise est bien équipée pour en tirer profit » et

qualifie ces bases de données ADN civiles de « prochaine étape logique ».

Qui est la NSCAI ?

Étant donné les changements radicaux aux États-Unis que prône la NSCAI dans cette présentation datant de mai dernier, il devient important d’examiner qui compose la commission et de considérer son influence sur la politique américaine, en particulier pendant la crise actuelle. Comme mentionné précédemment, le président de la

NSCAI est Eric Schmidt, l'ancien directeur d'Alphabet (la société mère de Google) qui a également beaucoup investi dans les entreprises technologiques israéliennes liées au renseignement, notamment dans la très controversée « incubateur » de start-up, la Team8. Le vice-président de la commission est Robert Work, qui est non seulement un ancien haut fonctionnaire du Pentagone, mais qui travaille actuellement avec le groupe de réflexion CNAS, dirigé par le conseiller de longue date en politique étrangère de John McCain et l'ancien conseiller à la sécurité nationale de Joe Biden.

Les autres membres de la NSCAI sont :

- Cafra Catz, PDG d'Oracle, qui entretient des liens étroits avec le principal donateur de Trump, Sheldon Adelson
- Steve Chien, superviseur du groupe d'intelligence artificielle au Jet Propulsion Lab de Caltech
- Mignon Clyburn, membre de l'Open Society Foundation et ancien commissaire de la FCC
- Chris Darby, PDG d'In-Q-Tel (la branche de la CIA spécialisée dans le capital-risque)
- Ken Ford, PDG de l'Institut de Floride pour la cognition humaine et mécanique

- Jose-Marie Griffiths, présidente de l’université d’État du Dakota et ancienne membre du Conseil national des sciences
- Eric Horvitz, directeur de Microsoft Research Labs
- Andy Jassy, PDG d’Amazon Web Services (contractant de la CIA)
- Gilman Louie, associé chez Alsop Louie Partners et ancien PDG d’In-Q-Tel
- William Mark, directeur de SRI International et ancien directeur de Lockheed Martin
- Jason Matheny, directeur du Center for Security and Emerging Technology, ancien directeur adjoint du renseignement national

et ancien directeur de l’IARPA (Intelligence Advanced Research Project Agency)

- Katharina McFarland, consultante chez Cypress International et ancienne secrétaire adjointe à la défense pour les acquisitions
- Andrew Moore, responsable de Google Cloud AI

Comme on peut le voir dans la liste ci-dessus, il existe un chevauchement considérable entre la NSCAI et les entreprises qui conseillent actuellement la Maison Blanche sur la « réouverture » de l’économie (Microsoft, Amazon, Google, Lockheed Martin, Oracle) et un

de ses membres, Safra Katz d'Oracle, fait partie du groupe de travail de la Maison Blanche sur la « relance économique ». Par ailleurs, il existe également un chevauchement entre le NSCAI et les entreprises qui sont intimement impliquées dans la mise en œuvre du « système de surveillance des coronavirus par recherche de contacts », un système de surveillance de masse promu par le groupe de travail sur les coronavirus du secteur privé, dirigé par Jared Kushner. Ce système de surveillance sera mis en place par des entreprises ayant des liens étroits avec Google et l'État américain de sécurité

nationale. Google et Apple, qui créent les systèmes d'exploitation de la grande majorité des smartphones utilisés aux États-Unis, ont déclaré qu'ils allaient désormais intégrer ce système de surveillance directement dans les systèmes d'exploitation de leurs smartphones.

Il convient également de noter qu'In-Q-Tel et la communauté américaine du renseignement sont très bien représentés au sein de la NSCAI et qu'ils se targuent également d'entretenir des liens étroits avec Google, Palantir et d'autres géants de la Silicon Valley,

ayant été les premiers à investir dans ces entreprises. Google et Palantir, ainsi qu'Amazon (également au sein de la NSCAI) sont également des contractants importants pour les agences de renseignement américaines. La participation d'In-Q-Tel à la NSCAI est également importante, car depuis plusieurs années, l'entreprise encourage fortement la surveillance de masse des appareils électroniques grand public destinés à être utilisés en cas de pandémie. Une grande partie de cette impulsion est venue de l'actuelle vice-présidente exécutive d'In-Q-Tel, Tara O'Toole, qui était auparavant directrice

du Johns Hopkins Center for Health Security et a également co-écrit plusieurs simulations controversées de guerre biologique et de pandémie, comme Dark Winter.

En outre, depuis janvier au moins, la communauté du renseignement américain et le Pentagone ont été à l’avant-garde de l’élaboration des plans d’intervention du gouvernement américain, toujours classés « style 11 septembre », pour la crise des coronavirus, aux côtés du Conseil national de sécurité. Peu d’organismes de presse ont noté que ces plans d’intervention classifiés, qui sont censés

être déclenchés si et quand les États-Unis atteindront un certain nombre de cas de coronavirus, ont été créés en grande partie par des éléments de l'État de sécurité nationale (c'est-à-dire le NSC, le Pentagone et les services de renseignement), sans participation des organismes civils ou de ceux qui se concentrent sur les questions de santé publique.

De plus, il a été rapporté que la communauté du renseignement américain ainsi que les services de renseignement militaires américains savaient au moins depuis janvier (et même des rapports plus récents disent

dès novembre dernier) que la crise du coronavirus atteindrait des « proportions pandémiques » en mars. Le public américain n’a pas été prévenu, mais l’élite des milieux d’affaires et de la classe politique a apparemment été informée, étant donné le nombre record de démissions de PDG en janvier et plusieurs allégations de délits d’initiés très médiatisées qui ont précédé la crise actuelle de quelques semaines.

Ce qui est peut-être encore plus déconcertant est le fait que le gouvernement américain n’a pas seulement participé à cette étrange simulation de pandémie d’octobre

dernier, connue sous le nom d’Event 201, mais qu’il a également mené une série de simulations de réponse à une pandémie, l’année dernière. Le projet Crimson Contagion était une série de quatre simulations qui impliquaient 19 agences fédérales américaines, y compris les services de renseignement et l’armée, ainsi que 12 états différents et une foule d’entreprises du secteur privé qui simulaient une pandémie de grippe dévastatrice ayant son origine en Chine.

Il était dirigé par l'actuel secrétaire adjoint du HHS, Robert Kadlec, qui est un ancien lobbyiste pour les militaires et les services de renseignement et un conseiller en « bioterrorisme » de la sécurité intérieure de l'ère Bush.

En outre, Kadlec et le Johns Hopkins Center for Health Security, qui a été intimement impliqué dans l'Event 201,

ont tous deux des liens directs avec l’exercice de guerre biologique controversé de juin 2001, « Dark Winter », qui prédisait les attaques à l’anthrax de 2001, attaques qui se sont produites quelques mois plus tard de manière inquiétante. Bien que les médias et le gouvernement se soient efforcés de rejeter la responsabilité des attaques à l’anthrax sur une source étrangère, on a découvert par la suite que l’anthrax provenait d’un laboratoire d’armes biologiques américain et l’enquête du FBI sur cette affaire a été largement considérée comme une opération de dissimulation, y compris par l’enquêteur

du FBI qui avait autrefois la charge de cette affaire.

Compte tenu de ce qui précède, il convient de se demander si ceux qui partagent la vision de la NSCAI ont vu très tôt dans la pandémie de coronavirus une occasion d'apporter les « changements structurels » qu'il avait jugés essentiels pour contrer l'avance de la Chine dans l'adoption massive de technologies basées sur l'IA, surtout si l'on considère que nombre des changements figurant dans le document de mai 2019 sont maintenant

rapidement mis en œuvre sous couvert de la lutte contre le coronavirus.

La vision de la NSCAI prend forme

Bien que le document de la NSCAI ait été rédigé il y a près d'un an, la crise du coronavirus a entraîné la mise en œuvre de nombreux changements et la suppression de nombreux obstacles « structurels » qui, selon la Commission, devaient être modifiés de manière drastique afin de garantir un avantage technologique sur la Chine dans le domaine de l'IA. L'abandon de l'argent liquide, qui a lieu non seulement aux États-Unis mais aussi à l'échelle

internationale, n’est qu’un exemple parmi d’autres.

Par exemple, en début de semaine, CNN rapportait que les épiceries envisagent maintenant d’interdire les achats en personne et que le ministère américain du travail a recommandé que les détaillants commencent à l’échelle nationale à « utiliser une fenêtre de type drive-in ou à proposer des ramassages en bordure de trottoir » pour protéger les travailleurs contre l’exposition au coronavirus. En outre, la semaine dernière, l’État de Floride a approuvé un plan d’achat en ligne pour les familles à faibles revenus utilisant le

programme d’assistance nutritionnelle supplémentaire (Supplemental Nutrition Assistance Program – SNAP). D’autres rapports ont fait valoir que la distanciation sociale à l’intérieur des épiceries est inefficace et met en danger la vie des gens. Comme mentionné précédemment, le document de la NSCAI de mai 2019 soutient que l’abandon des achats en boutique est nécessaire pour atténuer « l’avantage de la Chine en matière d’adoption [de la technologie] » et affirme également que « lorsque l’achat en ligne est littéralement la seule façon d’obtenir ce

que vous voulez, les consommateurs vont en ligne ».

Des rapports ont également fait valoir que ces changements dans les habitudes d’achat dureront bien au-delà du coronavirus, par exemple un article de Business Insider intitulé « La pandémie de coronavirus pousse plus de gens en ligne et changera à jamais la façon dont les Américains font leurs courses, selon les experts ». Les personnes citées dans l’article affirment que cet abandon des achats en boutiques sera « permanent » et déclarent également que « plus de gens essaient ces services qu’ils ne l’auraient fait sans ce catalyseur et

donne aux acteurs en ligne une plus grande chance d'acquérir et de conserver une nouvelle clientèle ». Un article similaire dans Yahoo ! News affirme que, grâce à la crise actuelle, « notre dépendance aux achats en ligne ne fera qu'augmenter parce que personne ne veut attraper un virus dans un magasin ».

En outre, la tendance à l'utilisation massive de voitures sans chauffeur a également connu un essor grâce au coronavirus, les voitures sans chauffeur effectuant désormais des livraisons à la demande en Californie. Deux sociétés, l'une chinoise et l'autre soutenue par la

SoftBank du Japon, ont depuis été autorisées à utiliser leurs véhicules à moteur sur les routes californiennes, et cette autorisation a été accélérée en raison de la crise du coronavirus. Le directeur général de Nuro Inc, la société soutenue par la SoftBank, a été cité par Bloomberg comme ayant déclaré que « la pandémie de Covid-19 a accéléré la nécessité pour le public de disposer de services de livraison sans contact. Notre flotte R2 est conçue sur mesure pour changer la nature même de la conduite et du mouvement des marchandises en permettant aux gens de rester chez eux en toute sécurité pendant que leurs

courses, médicaments et colis leur sont apportés. » Notamment, le document de la NSCAI de mai 2019 fait référence au réseau interconnecté des sociétés soutenues par la SoftBank, en particulier celles soutenues par son « Vision Fund », financé en grande partie par l'Arabie saoudite, comme formant « le tissu conjonctif d'une fédération mondiale de sociétés technologiques » destinée à dominer l'IA.

La Californie n'est pas le seul État à avoir commencé à utiliser des voitures sans chauffeur, puisque la clinique Mayo de Floride les utilise désormais aussi. « L'utilisation de l'intelligence

artificielle nous permet de protéger le personnel contre l’exposition à ce virus contagieux en utilisant la technologie de pointe des véhicules autonomes et libère le temps du personnel qui peut être consacré au traitement et aux soins directs des patients », a déclaré le docteur Kent Thielen, PDG de la Clinique Mayo de Floride, dans un récent communiqué de presse cité par Mic.

Tout comme les changements apportés aux achats en boutique à l’ère des coronavirus, d’autres rapports affirment que les véhicules à conduite autonome sont là pour rester. Un rapport publié

par Mashable s’intitule « Il a fallu une épidémie de coronavirus pour que les voitures à conduite autonome deviennent plus attrayantes » et commence par déclarer : « Soudain, un avenir rempli de voitures à conduite autonome n’est plus un rêve de science-fiction. Ce qui était autrefois considéré comme une technologie effrayante et incertaine par de nombreux Américains ressemble davantage à un outil efficace pour se protéger d’une maladie infectieuse qui se répand rapidement ». Il affirme en outre qu’il ne s’agit pas d’un « changement éphémère » dans les habitudes de conduite et un PDG de

technologie cité dans l'article, Anuja Sonalker de Steer Tech, affirme que « Il y a eu un net réchauffement vers une technologie sans contact et sans humain. Les humains sont des risques biologiques, les machines ne le sont pas. »

Un autre thème de la présentation de la NSCAI, la médecine IA, a également vu son étoile monter ces dernières semaines. Par exemple, plusieurs rapports ont vanté les mérites des plateformes de découverte de médicaments basées sur l'IA pour identifier des traitements potentiels contre les coronavirus. Microsoft, dont

le directeur du laboratoire de recherche fait partie de la NSCAI, a récemment investi 20 millions de dollars dans son programme « IA pour la santé » afin d'accélérer l'utilisation de l'IA dans l'analyse des données sur les coronavirus. En outre, la « télémédecine » – une forme de soins médicaux à distance – a également été largement adoptée en raison de la crise du coronavirus.

Plusieurs autres technologies axées sur l'IA ont également été adoptées plus largement grâce au coronavirus, notamment l'utilisation de la surveillance de masse pour la «

recherche des contacts » ainsi que la technologie de reconnaissance faciale et la biométrie. Un récent article du Wall Street Journal déclare que le gouvernement envisage sérieusement de recourir à la fois à la recherche de contacts par le biais de données de géolocalisation téléphonique et à la technologie de reconnaissance faciale afin de suivre les personnes susceptibles d'être atteintes du coronavirus. En outre, les entreprises privées – comme les épiceries et les restaurants – utilisent des capteurs et la reconnaissance faciale pour savoir combien de personnes, et lesquelles, entrent dans leurs magasins.

En ce qui concerne la biométrie, des chercheurs universitaires s'efforcent maintenant de déterminer si « les smartphones et les vêtements biométriques contiennent déjà les données dont nous avons besoin pour savoir si nous avons été infectés par le nouveau coronavirus ». Ces efforts visent à détecter précocement les infections à coronavirus en analysant « les horaires de sommeil, les niveaux d'oxygène, les niveaux d'activité et le rythme cardiaque » à partir d'applications pour smartphones comme FitBit et les montres intelligentes. Dans les pays autres que

les États-Unis, les cartes d’identité biométriques sont présentées comme un moyen de suivre ceux qui sont immunisés ou non contre le coronavirus.

En outre, un article publié dans The Edge affirme que la crise actuelle modifie les types de biométrie à utiliser, affirmant qu’un changement vers le balayage thermique et la reconnaissance faciale est nécessaire :

"À ce stade critique de la crise, toute solution intégrée de reconnaissance faciale et de balayage thermique doit être mise en œuvre facilement, rapidement et de manière rentable. Les travailleurs qui retournent dans les bureaux ou les usines ne doivent pas avoir à se démener pour apprendre un nouveau processus ou à se débrouiller avec les formulaires de déclaration. Ils doivent se sentir en sécurité et en bonne santé pour pouvoir travailler de manière productive. Il leur suffit de regarder l'appareil photo et de sourire. Les caméras et les scanners thermiques, soutenus par une solution basée sur le cloud et les protocoles logiciels appropriés, feront le reste."

Le concept de « *villes intelligentes* » bénéficie également de la crise du coronavirus, *Forbes* ayant récemment écrit que « *les villes intelligentes peuvent nous aider à combattre la pandémie de coronavirus* ». Cet article indique que « *les gouvernements et les autorités locales utilisent la technologie, les capteurs et les données de la ville intelligente pour retracer les contacts des personnes infectées par le coronavirus. En même temps, les villes intelligentes contribuent également aux efforts visant à déterminer si les règles de distanciation sociale sont respectées.* »

L’article contient également le passage suivant :

> *"... [L]e recours à des masses de capteurs connectés montre clairement que la pandémie de coronavirus est - intentionnellement ou non - utilisée comme banc d'essai pour les nouvelles technologies de surveillance qui peuvent menacer la vie privée et les libertés civiles. Ainsi, en plus d'être une crise sanitaire mondiale, le coronavirus est effectivement devenu une expérience sur la façon de surveiller et de contrôler les personnes à grande échelle."*

Un article du Guardian indique que « si l’un des enseignements du gouvernement sur le coronavirus est que les ‘villes intelligentes’, comme Songdo ou Shenzhen, sont plus sûres du point

de vue de la santé publique, nous pouvons nous attendre à des efforts accrus pour capturer et enregistrer numériquement notre comportement dans les zones urbaines – et à des débats acharnés sur le pouvoir que cette surveillance confère aux entreprises et aux États ». Certains rapports affirment également que les villes typiques sont « terriblement mal préparées » pour faire face aux pandémies par rapport aux « villes intelligentes ».

Cependant, au-delà des nombreuses préoccupations spécifiques de la NSCAI concernant l'adoption massive de l'IA, qui ont été résolues de façon pratique

par la crise actuelle, un effort concerté a également été fait pour changer la perception du public sur l’IA en général. Comme indiqué précédemment, la NSCAI avait souligné l’année dernière que :

> *"Dans la presse et la politique américaine et européenne, l’IA est dépeinte comme une personne à craindre qui érode la vie privée et vole des emplois. À l'inverse, la Chine la considère à la fois comme un outil pour résoudre les grands défis macroéconomiques afin de pérenniser son miracle économique, et comme une opportunité de prendre le leadership technologique sur la scène mondiale."*

Aujourd’hui, moins d’un an plus tard, la crise du coronavirus a contribué à faire la une de nombreux journaux au cours des dernières semaines qui se mettent à décrire l’IA de manière très différente, notamment « Comment l’intelligence artificielle peut aider à lutter contre le coronavirus », « Comment l’IA peut prévenir la prochaine épidémie de coronavirus », « L’IA devient un allié dans la lutte contre le COVID-19 », « Coronavirus : l’IA se dresse contre le COVID-19 » et « Voici comment l’IA peut aider l’Afrique à lutter contre le coronavirus », parmi de nombreux autres titres.

Il est en effet frappant de constater à quel point la crise du coronavirus semble avoir rempli toute la liste de souhaits de la NSCAI et supprimé de nombreux obstacles à l'adoption massive des technologies de l'IA aux États-Unis. À l'instar des grandes crises du passé, l'État de sécurité nationale semble utiliser le chaos et la peur pour promouvoir et mettre en œuvre des initiatives qui seraient normalement rejetées par les Américains et, si l'on en croit l'histoire, ces nouveaux changements se poursuivront longtemps après que la crise du coronavirus se sera

estompée du cycle des nouvelles. Il est essentiel que ces soi-disant « solutions » soient reconnues pour ce qu'elles sont et que nous réfléchissions au type de monde qu'elles finiront par créer – une technocratie autoritaire. Nous ignorons l'avancée rapide de ces initiatives promues par la NSCAI et l'élimination progressive des systèmes dits « culturels » (et avec eux, de nombreuses libertés tant désirées) à nos propres risques et périls.