

Europe's Digital Decade?

Navigating the global battle
for digital supremacy

Clingendael Report

Brigitte Dekker
Maaïke Okano-Heijmans



Clingendael

Netherlands Institute of International Relations



Clingendael

Netherlands Institute of International Relations

Europe's Digital Decade?

Navigating the global battle for digital supremacy

Brigitte Dekker
Maaïke Okano-Heijmans

Clingendael Report
October 2020

Disclaimer: The research for and production of this report has been conducted within the PROGRESS research framework agreement. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, nor should be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defence.

October 2020

Cover photo: Global business concept. Network of business. Diversity. © Shutterstock

Unauthorized use of any materials violates copyright, trademark and / or other laws. Should a user download material from the website or any other source related to the Netherlands Institute of International Relations 'Clingendael', or the Clingendael Institute, for personal or non-commercial use, the user must retain all copyright, trademark or other similar notices contained in the original material or on any copies of this material.

Material on the website of the Clingendael Institute may be reproduced or publicly displayed, distributed or used for any public and non-commercial purposes, but only by mentioning the Clingendael Institute as its source. Permission is required to use the logo of the Clingendael Institute. This can be obtained by contacting the Communication desk of the Clingendael Institute (press@clingendael.org).

The following web link activities are prohibited by the Clingendael Institute and may present trademark and copyright infringement issues: links that involve unauthorized use of our logo, framing, inline links, or metatags, as well as hyperlinks or a form of link disguising the URL.





About the authors

Brigitte Dekker is a Research Fellow at the Netherlands Institute of International Relations 'Clingendael' in The Hague. Her research focuses on various dimensions of EU-Asia relations, with a specific interest in South-East Asia and China.

Maaïke Okano-Heijmans is a Senior Research Fellow at the Netherlands Institute of International Relations 'Clingendael' in The Hague and a visiting lecturer at the University of Leiden.

The Clingendael Institute
P.O. Box 93080
2509 AB The Hague
The Netherlands

Follow us on social media

 @clingendaelorg
 The Clingendael Institute
 The Clingendael Institute
 clingendael_institute

Email: info@clingendael.org
Website: www.clingendael.org

Table of contents

Executive summary	1
1 Introduction	3
Where does Europe stand today?	4
2 Regulation	7
2.1 Personal data flows	9
International context	9
Regional focus: South-East Asia	10
The EU–US Privacy Shield	11
Moving forward	11
2.2 Non-personal data flows	12
2.3 The multilateral context: the WTO	13
3 Business: e-commerce, the platform economy and digital payments	15
3.1 E-commerce	15
3.2 Platform economy	18
International efforts on e-commerce and platform regulation	19
The EU’s turn from defensive to offensive measures?	21
3.3 Digital payments	21
3.4 The multilateral context: the WTO and OECD	23
The Organisation for Economic Cooperation and Development	24
4 Telecommunications infrastructure	25
4.1 5G networks: the embodiment of US–China tech rivalry	25
Asia–Pacific: a region to watch	26
4.2 Cloud computing	28
4.3 The multilateral context: the ITU and beyond	29
5 Conclusion	32
Annexe 1	35
List of abbreviations	37

Executive summary

On 16 September 2020, European Commission President Ursula von der Leyen set a clear goal for the European Union (EU) and its member states when she said that ‘Europe must now lead the way on digital – or it will have to follow the way of others, who are setting these standards for us’. She added: ‘We must make this [‘Europe’s Digital Decade’](#)’.

Many in Brussels acknowledge today that the half page on digital matters in the EU connectivity strategy needs to be operationalised and put into action. Efforts to strengthen Europe’s industrial and digital strategies at home are already being made. Yet joint, coherent action by EU institutions and stakeholders within member states are needed not just within the Single Market, but also in and with third countries and in international networks and institutions.

Central to the debate and any policy decision on digital connectivity are the trade-offs concerning privacy, business interests and national security. While all regulations are a combination of these three, the United States (US) has taken a path that prioritises the interests of businesses. This is manifested, for example, in the strong focus on free data flows, both personal and non-personal, to strengthen companies’ competitive advantage in collecting and using data to develop themselves. China’s approach, by contrast, strongly focuses on state security, wherein Chinese businesses are supported and leveraged to pre-empt threats to the country and, more specifically, to the Chinese Communist Party. This is evident from its strict data localisation requirements to prevent any data from being stored outside its borders and a mandatory security assessment for cross-border transfers. The European Union represents a third way, emphasising individuals’ privacy and a human-centred approach that puts people first, and includes a strong focus on ethics, including in data-protection regulations.

This Clingendael Report aims to increase awareness and debate about the trade-offs of individual, state and business interests in all subsets of digital connectivity. This is needed to reach a more sustainable EU approach that will outlast the present decade. After all, economic competitiveness is required to secure Europe and to further its principled approach to digital connectivity in the long term. The analysis presented here covers a wide range of topics within digital connectivity’s three subsets: regulation; business; and telecommunications infrastructure. Aiming to contribute to improved European policy-making, this report discusses (best) practices of existing and rising digital powers in Asia and the United States. In every domain, potential avenues for cooperation with those countries are explored as ways forward for the EU.

Findings show that the EU and its member states are slowly but steadily moving from being mainly a regulatory power to also claiming their space as a player in the digitalised world. Cloud computing initiative GAIA-X is a key example, constituting a proactive alternative to American and Chinese Cloud providers that is strongly focused on uniting small European initiatives to create a strong and sustainable Cloud infrastructure. Such initiatives, including also the more recent Next Generation Internet (NGI), not only help defend and push European digital norms and standards, but also assist the global competitiveness of European companies and business models by facilitating the availability of large data-sets as well as scaling up. Next to such 'EU only' initiatives, working closely together with like-minded partners will benefit the EU and its member states as they seek to finetune and implement their digital strategies. The United States and Asian partners, particularly Japan, South Korea, India and Singapore, are the focus of attention here. This report thereby offers clues for a policy agenda as well as concrete suggestions for enhancing cooperation in the digital domain between the EU and like-minded partners.

1 Introduction¹

In her [State of the Union speech](#) of September 2020, European Commission President Ursula von der Leyen highlighted the need for ‘a common plan for digital Europe with clearly defined goals for 2030, such as for connectivity, skills and digital public services’. The Commission President called for a principled approach, focusing on the right to privacy and connectivity, freedom of speech, free flow of data and cyber security.

COVID-19 has laid bare the risks of failing to act on the ‘digital decade’. The pandemic has put on full display the profound and disrupting impact of digitalisation on domestic societies and international relations. The protection of digital freedom of speech, transparency and inclusiveness is at stake as governments resort to (sometimes intrusive) digital means to monitor and combat the virus. At the same time, upholding economic competitiveness in the digital age requires innovative approaches to research, development and – in particular – commercialisation of innovation.

The pandemic reaffirmed the need for improved resilience at home as well as cooperation among like-minded partners that wish to uphold an open and inclusive cyber domain. For the EU and its member states, this requires an update – that is, a broadening and deepening – of the digital dimension of the EU’s connectivity strategy of 2018, with clear links to the 2020 EU Digital Strategy. Options for EU action are defined and confined by the US–China technology rivalry, which is reshaping the global tech landscape and global governance, including in the digital field.

This report aims to contribute to such an updating of the digital dimension of the EU connectivity strategy. It analyses what is at stake for the EU and its member states in the field of digital connectivity – specifically, its subsets of regulation, business and telecommunications infrastructure. Aiming to contribute to a principled but sustainable approach to the digital field, as well as improved European policy-making, it discusses (best) practices of existing and rising digital powers in Asia and the United States. In every domain, potential avenues for cooperation with those countries are explored as ways forward for the EU. Finally, the report offers clues for a policy agenda as well as concrete suggestions for enhancing cooperation in the digital domain between the

1 The authors wish to acknowledge the valuable research assistance provided by Eric Siyi Zhang throughout his internship at the Clingendael Institute, from March–July 2020. They also express their appreciation to all interviewees and reviewers at EU institutions, Dutch ministries and companies, and multilateral institutions who generously shared their insights.

EU and like-minded partners. These are crucial steps to take if the EU and its member states are to make this [‘Europe’s Digital Decade’](#), as proposed by Ursula von der Leyen.

Where does Europe stand today?

The European Commission led by Ursula von der Leyen acted on the digital challenge with the adoption in February 2020 of the strategy [A Europe fit for the digital age](#). This strategy provides a strong foundation for European competitiveness in the so-called Fourth Industrial Revolution² and aims to strengthen the strategic autonomy of Europe.³ It builds on ongoing efforts to create an EU [Digital Single Market](#), providing practical guidelines and regulations to take the EU’s efforts to the next stage in the field of digitalisation. The focus on digitalisation in the forthcoming [Multiannual Financial Framework \(MFF\)](#), including the extra allocation of €750 billion for a new recovery programme called ‘Next Generation EU’, shows that the EU is now ready to prioritise digitalisation to create the funding necessary to back up the EU’s digital strategy.

The EU’s digital strategy is [divided into four pillars](#): technology that works for people; the digital economy; digital society; and a digital global perspective. The contours of this fourth element – that is, the international context to digital policy-making – were touched upon earlier in the [EU strategy on connecting Europe and Asia](#) of September 2018. This so-called ‘connectivity strategy’ highlights the importance of digital connectivity in an increasingly globalised world, along with transport, energy and human connectivity. On paper, the EU seems ready to act on connectivity in the digital age, but in practice, it is stumbling along. As many in Brussels acknowledge, the half page on digital policy in the EU connectivity strategy needs to be operationalised and put into action through joint, coherent efforts by EU institutions and member state stakeholders, as well as in multilateral institutions and in coordination with (networks of) like-minded partners.

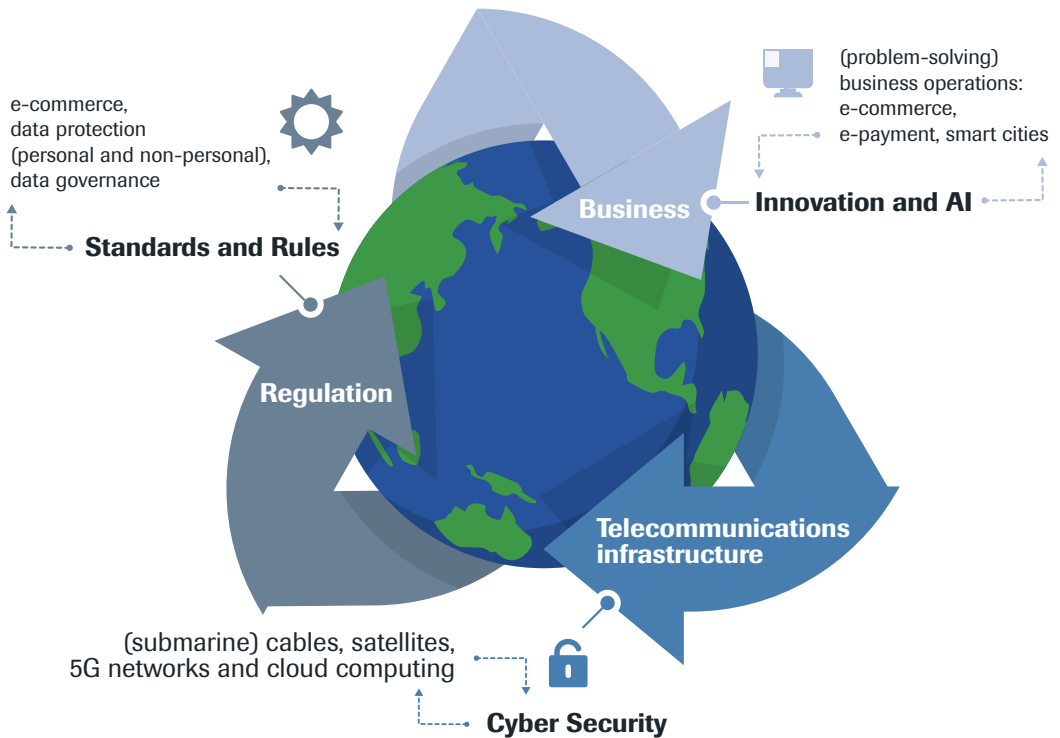
Now, as the impact of COVID-19 is still unfolding and the US–China tech-data rivalry is intensifying, the EU and its member states need to unpack, instrumentalise and act upon digital connectivity. The broad domain of digital connectivity can be divided into three categories that are not mutually exclusive and [have significant overlaps in practice](#). As visualised in Figure 1, these categories are: regulation (standards and rule-setting in data governance); business (the global race for supremacy in innovation and artificial

2 Following mechanisation thanks to steam and water, mass production enabled by electricity, and automation owing to digital tools including the Internet, the fourth industrial revolution is now facilitating robotisation by way of integrating information and communications technology (ICT) in all of society.

3 [Strategic autonomy](#) refers to both the ability to be autonomous – not dependent on – of other powers and the ability to decide autonomously and to act freely in an interdependent world.

intelligence (AI), but also e-commerce and e-finance); and (tele)communications infrastructure (cyber security). All of these categories must be tackled at home (within the EU) and in third countries, and can benefit from cooperation and coordination with (like-minded) partners as well as be strengthened by digital official development assistance (ODA).

Figure 1 Digital connectivity's three categories: strategic and practical levels



Source: adjusted from Okano-Heijmans (2019).

International cooperation and synergies are essential to further rule-based global governance that underpins the e-economy, technical innovation and the cyber domain. As well as cooperation in institutions, coordination is needed to optimise outcomes and enhance synergies, as major geo-economic powers push forward digital initiatives and strategies of their own, such as China's Digital Silk Road, the United States' Digital Connectivity and Cybersecurity Partnership (DCCP) and the Association of South-East Asian Nations' (ASEAN's) Masterplan on Connectivity.

The rapidly digitalising Asian economies – especially China, India, Japan, Singapore and South Korea – are of strategic importance for all great powers, as access to and influence on their digital infrastructures and dataflows may tip the balance in the race for digital supremacy. Best-practice learning and engagement with these Asian countries in digital alliances will contribute to greater resilience at home and the promotion of European interests, norms and standards abroad. China's efforts in the digital domain, and the challenges and opportunities these pose to Europe are of key importance here. They are detailed in the July 2020 Clingendael Report [Unpacking China's Digital Silk Road](#) (DSR).

This report complements the July 2020 report on China's DSR, as well as a May 2020 Clingendael Policy Brief on so-called [digital ODA](#). This report focuses on the approaches of Asian countries and the United States in the digital sphere. Comparing these to European practices, our ultimate aim is to highlight opportunities for synergies, cooperation and coordination with the EU and its member states, for the sake of an open, inclusive and transparent digital future.

2 Regulation

Regulation in the field of digital connectivity mainly concerns the cross-border movement of personal and non-personal data, as well as e-commerce and cyber governance. This section assesses the state of play in the field of personal and non-personal data, comparing the EU's approach to that of other key players.⁴ Today, variations in the approaches and frameworks of the EU, United States, China and other Asian players hamper the interoperability of systems in the various economies. Better understanding of existing regulations and the norms and values underpinning them is imperative as the EU and its member states define their own approach. At the multilateral level, the World Trade Organisation (WTO) plays a key role in writing new rules for the digital economy – in particular for e-commerce.

Central to the legislative processes of general data regulations is the trade-off concerning privacy, business interests and state security. While all regulations cover a combination of these three, the United States has taken a path that clearly prioritises the interests of businesses. This is manifested in its strong focus on free data flows, both personal and non-personal, to strengthen companies' competitive advantage in collecting and using data to develop themselves. The US approach contrasts with China's approach, which prioritises state security, [mobilising all of society](#) to pre-empt threats from both inside and outside China's borders. The Chinese Communist Party is leveraging state-owned enterprises, Chinese technology companies and partnerships with foreign partners for this purpose. This is evident from China's strict data localisation requirements to prevent any data from being stored outside China's borders and a [mandatory](#) security assessment for cross-border transfers. The EU represents a third way, emphasising individuals' privacy and a human-centred⁵ approach to data-protection regulations – a perspective that puts people first and includes a strong focus on ethics.

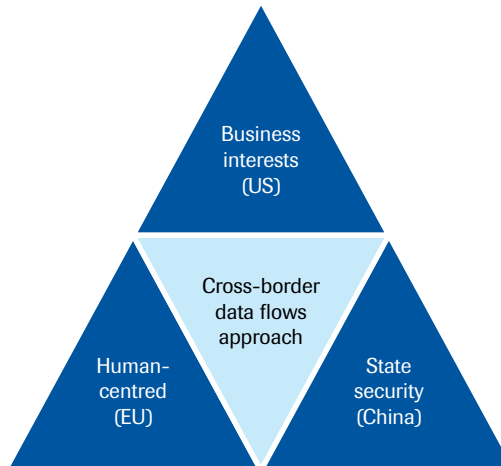
The disparity of the major players' approaches, as visualised in Figure 2, complicates cross-border data flow and international agreements to smooth such flows. The approaches are incompatible and represent a trade-off concerning the interests of the individual, the company and the state. Currently, the General Data Protection

4 A more in-depth analysis on cyber governance can be found in our August 2020 Clingendael report: ['Unpacking the Digital Silk Road'](#).

5 Internationally, the term *human-centric* – focusing on human beings – is used more often. However, in this context, *human-centred* seems to be more appropriate, as it includes humanistic values and devotion to human welfare as well.

Regulation (GDPR) hampers the EU's potential to innovate, as most innovation in new technologies such as artificial intelligence (AI) is dependent on large data sets. Competitors from the United States and China had already built such data sets before the GDPR was in place and thus now have more freedom to invest and innovate. To address this problem, the [EU data strategy](#) – as part of the EU digital strategy – includes the commitment to pool European data in key sectors, to create interoperable data spaces. More awareness and debate about the trade-offs of individual, state and business interests are needed to reach a more balanced EU approach.

Figure 2 Approaches to data regulation: prioritising privacy, business interests and state security



To create more compatibility and a global standard for data regulations, the EU can partner with like-minded Asian countries. Many of these countries are in the process of drafting their own data regulations, while utilising the existing frameworks, including the GDPR. Shared concerns about the United States and China offer a good incentive to bring data-protection regulations closer together. Presenting a human-centred approach focused on privacy may inspire regulations based on the needs of the growing digital environment in many Asian countries. Internationally, a synchronised data approach between the EU and Asian countries would add leverage to the much broader global debate on digitalisation and the use of data for innovation and national security.

2.1 Personal data flows

With the GDPR, the EU took a strong normative stance to protect citizens' data and privacy, while also ensuring the free flow of personal data within the Union and [prohibiting](#) data localisation requirements. The GDPR⁶ is a catch-all regulation that elevates the protection of personal data to a fundamental right protected by a [comprehensive legal standard](#). The EU hereby set new standards for any [holder of sensitive data about EU citizens](#), within the EU and beyond.

The global debate on cross-border data flows and data protection accelerated rapidly because of the GDPR's extra-territorial scope, meaning that the regulation applies to foreign companies located outside EU borders that are processing EU citizens' data. This has made the EU a standard-setter in the field and triggered a global debate about privacy as a digital human right. Now, a growing number of countries outside Europe – including India, Thailand, Chile and Australia – are also drafting or implementing (personal) data flow regulations – oftentimes inspired by the EU's action.

Yet despite all its merits, the GDPR comes at a cost – a cost to European economic competitiveness. In prioritising individual privacy, the GDPR obstructs data-gathering by companies. This, in turn, applies a brake to digital innovation, companies' growth perspectives and commercial practices, which rely heavily on the availability of large data sets. Whereas big US technology firms, in particular, built large data sets in the years before the GDPR was in place, European start-ups and small- and medium-sized companies are struggling to build them and are thereby having great difficulty in competing internationally.

International context

Since [2016](#), the EU has linked intra-EU data protection with the external dimension through adequacy decisions – that is, the European Commission can review whether a non-EU country offers an adequate level of protection. If deemed adequate, a company's data from this country will be handled as if it is located within an EU member state.⁷ However, as all data have to adhere to the (high) European standards, not many countries are granted the status of an adequate country. For example, India applied but

6 Companies and organisations have to comply with the [GDPR](#) to ensure that EU citizens have the required level of control over the collected personal information. The GDPR does not apply to 'purely personal or household activity', or small and medium-sized organisations with fewer than 250 employees if those are located outside the EU.

7 So far, Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield Framework) have been recognised as providing [adequate protection](#).

was rejected, and adequacy talks with [South Korea](#) are still ongoing, since its domestic legislation had to be amended – which [happened](#) in January 2020. Japan obtained its [adequate status from the EU in January 2019](#).

Internationally, both the [United States](#) and [China](#) take a different stance than the EU, with legislation that has no [extra-territorial scope](#) and focuses on, respectively, commercial interests and state security, rather than consumer interests. Annexe 1 (see the end of this report) schematically presents the similarities and differences between the various frameworks. For its part, India (the largest emerging digital economy) prioritises data localisation, thus aiming to [limit data exploitation](#) by foreign multinationals. Nevertheless, the frameworks of China and India are comparable to the GDPR, with different levels of protection for defined types of data, and different wording and scope. Complementing national legislation in many countries, various frameworks and initiatives have emerged, such as the Cross-Border Privacy Rules (CBPR) system of the Asia-Pacific Economic Cooperation (APEC), the ASEAN data protection forum, the EU-US Privacy Shield and the Data Free Flow with Trust (DFFT). The DFFT focuses primarily on company data, while all the others are concerned with consumer data. APEC's CBPR, the EU-US Privacy Shield and the DFFT will be elaborated upon below.

Regional focus: South-East Asia

A focus on privacy and data protection is still nascent in South-East Asia and countries are catching up unevenly. APEC's [CBPR system](#) is a government-backed data-privacy certification that companies can join to demonstrate compliance with internationally recognised data-privacy protections.

APEC's voluntary, certification-based approach to personal data regulation offers an alternative, less legalistic mode of regulation than Europe's GDPR. While the 21 APEC economies together developed the CBPR, only eight countries joined the system: Australia, Taiwan, Canada, Japan, the Republic of Korea, Mexico, Singapore and the United States. The CBPR has already found its way into the revised [North American free-trade agreement](#), also known as the United States-Mexico-Canada Agreement (USMCA). In addition, the United States is now [citing](#) APEC's CBPR – rather than the GDPR – to manage data transfers between the United States and the United Kingdom (UK) after Brexit. That said, several APEC members in South-East Asia that do have national privacy and data-protection laws are streamlining their laws and policies also with the GDPR.⁸ As these countries offer a huge market in terms of economic

⁸ [For example](#), Malaysia is reviewing its Personal Data Protection Act of 2010 to streamline it with the GDPR; Singapore shares many GDPR principles; the Philippines are mirroring GDPR policies; Thailand passed an Act offering citizens similar protection to the GDPR; Indonesia, Laos, Vietnam, Cambodia, Myanmar and Brunei currently do not have data protection laws.

activity and potential transfers of data, it would benefit the EU if they adopt GDPR-like regulations. This would certainly make potential adequacy talks – and, subsequently, access to the ASEAN data – easier and would unleash further potential for future cooperation.

The EU–US Privacy Shield

While the CBPR can be adopted on a voluntary basis, the EU–US Privacy Shield is a mandatory agreement between the EU and the United States, guaranteeing that foreign (in this case US) businesses handle EU data in line with EU regulations, in return for unrestricted data flows. This Privacy Shield was introduced when transatlantic data flows were threatened by the non-adequacy status of the United States in 2016, after the European Court of Justice ruled the earlier [Safe Harbour agreement invalid](#) and required that US companies sign up to higher privacy standards and [uphold similar levels](#) to EU privacy protection. By 2020, the Privacy Shield [underpinned US\\$7.1 trillion](#) of transatlantic digital trade and was used by more than [5,300 companies](#).

While the Privacy Shield seemed to be a promising tool to smooth transatlantic trade, the European Court of Justice in mid-July 2020 [invalidated](#) the Shield as well, noting that the privacy of users could not be guaranteed in the United States. Especially US intelligence services could easily request the EU data, thereby violating the EU GDPR. Now, EU companies have to review their third parties' data flows and contracts, specifically US Cloud providers, to check which data is suddenly unlawfully transferred to the United States. The US Department of Commerce's International Trade Administration [continues to administer](#) the Privacy Shield programme. The difficulty with the July 2020 ruling is that no alternative to the Privacy Shield is yet available for transatlantic data flows. Even though global companies can still [operate](#) because of contractual clauses that are considered sufficient to protect data transfers, no clear standards to guide them are available. For the EU, it will be hard to [protect citizens' data](#) and at the same time support the creation of economies of scale while upholding strict privacy standards. Companies still transferring data will be in [a delicate position](#) once US authorities request their data for national security purposes, leaving companies with the choice of fighting this US decision or facing [fines of up to 20 million euros](#) in the EU.

Moving forward

As the EU–US Privacy Shield is being dissolved, the EU has to reposition itself in the global discussion on personal data transfers. The United States is unlikely to start adequacy talks and the United Kingdom is already leaning towards endorsing APEC's CBPR after Brexit. In Asia, Japan is an interesting player for discussions about future steps. Japan recently acquired the status of adequate country with the EU, while it is also one of the eight countries endorsing the CBPR framework. Hence, the systems can be implemented simultaneously, ensuring the protection of citizens' data in

the EU and beyond. The CBPR does not require any national laws to be amended; states and individual companies only have to ensure a [baseline of privacy protection](#). After successful adaptation to CBPR regulations, the EU can present the GDPR as an extensive addition to the CBPR framework.

South Korea also stands out as an interesting partner for the EU. South Korea has also endorsed the CBPR and has been adjusting national laws in 2020 to acquire adequacy status from the EU. Moreover, Seoul's strategy more broadly dovetails perfectly with the EU's [digital strategy](#) and [EU green deal](#). It is based on two pillars: the [Digital New Deal](#), which aims to create an inclusive digital economy based on values that put people first and improve quality of life; and the [South Korean Green New Deal](#). Combined with South Korea's ongoing adequacy talks with the EU, increased dialogue between South Korea and the EU at governmental and business levels is likely to contribute to further cooperation in digitalisation and digital green initiatives.

2.2 Non-personal data flows

To unleash the full potential of an EU Single Digital Market, the EU in 2019 also adopted regulation on the free flow of [non-personal data](#). [This free flow of data regulation \(FFD\)](#) comprises, for example, business or industrial data, and raw machine data. The EU [defines](#) non-personal data as 'data other than personal data'. This includes, for example, weather conditions generated by sensors, data on maintenance needs for industrial machines, or data that were initially personal data, but are anonymised in such a way that they cannot be attributed to a specific person, even if additional data are used.

Together with the GDPR on personal data, the EU's FFD amounts to a comprehensive approach to data regulation that creates legal certainty for companies and guarantees that [personal and non-personal data](#) can move freely within the EU. The free flow of non-personal data [intends to help companies](#), especially small and medium-sized companies and start-ups, to scale up more easily and enter new markets. [Central to the FFD](#) are the prohibition of data localisation restrictions for member states, the prevention of vendor lock-in, preventing legal uncertainty among governments and companies regarding cross-border data storage and processing, and increasing trust to address security risks and concerns in a timely and adequate manner.

In order to facilitate the free flow of such non-personal data also beyond EU borders, the EU supports the global initiative towards the [Data Free Flow with Trust \(DFFT\)](#) – a framework to create a free zone for the flow of 'medical, industrial, traffic and other most useful, non-personal, anonymous data'. International cooperation is necessary, as the proliferation of laws restricting data flows (so-called 'data localisation') may result in a reduction of cross-border business or even a protectionist race to the bottom with regimes [trying to attract or retain economic activity](#) in their jurisdiction.

The DFFT Initiative was launched by Japanese Prime Minister Abe at the January 2019 World Economic Forum in Davos. In June 2019, seventeen of the G20 leaders – including China, but excluding India, South Africa and Indonesia – endorsed the [G20 Osaka Leaders' Declaration](#), including the [section](#) on 'Innovation: Digitalisation, Data Free Flow With Trust'.

When combining the regulatory powers of the EU and Japan, the two economic giants can be a powerful force pushing for a comprehensive approach to global (non-)personal data regulation. At the EU–Japan summit of May 2020, the two powers [emphasised](#) the need for joint efforts to elaborate further the DFFT and facilitate safe and secure cross-border data flows. This laid an important foundation for greater engagement and cooperation, also with other economies in the Asian region and beyond.

China's endorsement of the DFFT is noteworthy, because Beijing is known for its [strict digital protectionism](#), as shown in the cross-border data flow constraints and active filtering of websites deemed to pose a threat to the Chinese Communist Party. Chinese President Xi Jinping mentioned on several occasions that data is the equivalent of '[what oil is to the industrial economy](#)', thereby emphasising China's power generated by its 'oil field' of data. Combined with Beijing's strict cross-border data provisions, this is reason to question China's endorsement of the DFFT and to keep a close eye on any new data provisions – either cross-border transfers or new data localisation provisions – in the near future.

2.3 The multilateral context: the WTO

Considering its general objectives of liberalising trade, lowering trade barriers and facilitating trade without discrimination, the World Trade Organisation (WTO) stands out as the designated international organisation to address the emerging problems at the nexus of trade, innovation and data transfers. The introduction of new data-protection regulations in many countries and stricter control on cross-border data flows globally are raising concerns about whether such new regulations negatively affect transnational trade. Despite some [built-in flexibilities](#) such as transitional implementation periods, technical assistance and pre-commitments, the WTO does not yet provide a comprehensive mechanism to manage trade in personal data and the General Agreement on Trade in Services (GATS) – under which personal data is considered – does not provide any [clear guidelines](#). Therefore, the WTO now faces the question of how to balance the importance of the right to data privacy and the interests of trade.

The core general obligation under GATS is [the Most-Favoured Nation \(MFN\) treatment](#), which aims to eliminate formal and informal discrimination between countries concerning trade in services. In this context, member states' domestic restrictions on cross-border data transfers are considered potential discriminatory practices under the

WTO's MFN clause. Harmonisation of data-protection standards would thus be in line with the WTO's aim and the general obligation under GATS.

Set against this context, the DFFT was expected to reinvigorate WTO talks on cross-border data transfers. It tries to carve out a multilateral path to harmonise and mutually recognise privacy regimes, thereby [preventing fragmented economies](#). However, the multitude of views on data protection – specifically from the EU, the US and China – complicates discussions. Especially the interwovenness of trade, possible discrimination and questions about a country's sovereignty to regulate the domestic supply of services create an enormous challenge to continuing talks on a multilateral level. The EU [took](#) a strong stance when introducing the GDPR, providing citizens with a form of sovereignty over their own personal data. Moreover, China also made clear its position by introducing the concept of '[cyber sovereignty](#)' – to limit unwanted foreign influence in its cyberspace and to allow the Chinese government to continue its 'Great Firewall' and data localisation policies. Russia quickly adopted the use of the same concept to justify its [push](#) for a domestic internet, and the United States still advocates for free and open cyberspace to maximise business potential.

Creating synergies between the different stances to cross-border data flows will be an immense – if not impossible – task for the WTO. The leadership shown by Japan and the endorsement of the DFFT by at least seventeen of the twenty G20 countries do provide some hope that a minimum consensus can be reached within the WTO. A WTO initiative led by Japan and supported by the EU and South Korea would create a strong basis to push for global consensus on data transfer guidelines that balance citizens' privacy with also business interests and national security concerns.

3 Business: e-commerce, the platform economy and digital payments

Looking at the business side of digital connectivity – the global digital economy – three prominent elements need to be discussed: e-commerce; the platform economy; and digital payments. Global competition for innovation and the commercialisation of research and development (R&D) in the high-tech sector are relevant to each of these fields.

Remarkably, EU member states have the talent to compete with the United States and China on AI and [rank high on research](#), but [lag in commercial AI adoption](#) and funding. Hence, they now need to catch up with the US and China, which are homes to the big technology players: Google, Apple, Facebook, Amazon and Microsoft (GAFAM); and Baidu, Alibaba and Tencent (BAT), respectively. Following a discussion of where Europe stands in this field, including in comparison with like-minded countries, this section explores international efforts to level the playing field, as well as promising areas for cooperation by the EU with like-minded partners.

3.1 E-commerce

The European market has become [deeply integrated](#) into global markets through digitalisation, modern transport and communication means. Home to more than 500 million consumers with high purchasing power and looking for quality goods, combined with a high level of both physical and digital connectivity, the EU harbours great potential to develop competitive e-commerce businesses. Internally, the EU has made efforts to create a Digital Single Market and improve regulation concerning e-commerce since 2015.

For e-commerce to be successful and efficient, both physical and digital connectivity and data are crucial. Users have to be connected to the internet and willing to shop online.⁹ In the EU, [more than](#) 85 per cent of households had access to the internet in 2018, and 60 per cent of individuals aged 16 to 74 ordered goods from the internet in

9 Majcherczyk and Bai (2019). 'Digital Silk Road: The Role of Cross-Border E-Commerce in Facilitating Trade Global Economic Governance'. *Journal of WTO and China*, 9(2), p. 109.

2018 across the EU. For scaling up e-commerce businesses, physical connectivity may be just as important as digital connectivity, because without a good logistics system, companies cannot deliver goods to their customers on time and up to standards. Within the EU, the logistical systems [are satisfactory](#), but the complexity of cross-EU member state ordering and shipping restrains companies from growing European-wide. Moreover, data is the intangible resource without which e-commerce companies cannot provide high-quality and personalised service to their customers.

Noteworthy in e-commerce are the measures against [unjustified geo-blocking](#) (that is, prohibiting online customers from purchasing products or services on another EU member state's website), which entered into force in 2018. Unjustified geo-blocking reduces revenues for companies and choices for customers, and needs to be ended to unleash fully the potential of the Digital Single Market for European e-commerce companies. Also, the EU aims to create effective ways to regulate non-EU e-commerce companies that operate within the EU market, especially to [tax effectively all e-commerce companies selling in the EU](#). Current tax rules are outdated for the digital age of the global economy and fail to ensure fairness of competition. Multilateral efforts on new tax regimes will be detailed in section 3.4 below.

The largest e-commerce marketplaces in Europe are Amazon, E-bay and AliExpress – that is, US and Chinese companies. These companies are both e-commerce providers as well as comprehensive platforms offering a wide array of services, such as video and music streaming and payments. The largest European e-commerce business is German web shop Otto, part of Otto Group, which offers approximately 1.8 million items from about 6,800 brands in various categories. Otto's online turnover was approximately €13.7 billion in 2018 – still [less than half](#) of that of Amazon in Europe. The biggest challenge for European competitors from the US and Chinese marketplaces is their [national focus](#). Consider, for example, Allegro, which is the fifth most visited marketplace in Europe, but mostly focuses on Poland; and Bol.com, which was voted most popular retailer among Dutch consumers but does not operate beyond the Netherlands and Belgium.

The Franco-German initiative [GAIA-X](#) (described in detail in section 4.2 below) acts on this challenge of a splintered European market. This Cloud computing initiative aims to develop a secure data infrastructure that also allows for the development of innovative products and helps European companies and business models to scale up and be globally competitive. As well as furthering data sovereignty by offering European Cloud service infrastructure, GAIA-X increases the availability of large data sets in Europe. This, in turn, facilitates the scaling up of European companies and business models, and a strengthening of their innovative edge.

Hence, the global and even European presence of EU member states' e-commerce companies is negligible compared to Amazon, E-bay and AliExpress. The nationally

popular e-commerce companies are vulnerable to these global competitors that are slowly but steadily entering the European market. National e-commerce companies such as Allegro and Bol.com have already gained the trust of national customers, and experts therefore expect a switch of preference only if new e-commerce companies offer [at least a 10 per cent price drop](#) compared to the national alternatives. To protect homegrown companies, European regulators – led by the EU's competition commissioner Margrethe Vestager – are looking into anti-trust concerns about Amazon. The question of whether Amazon [uses sales data](#) from third-party merchants to adjust and boost the sales of Amazon's own products is particularly worrying for the EU. [Italy and Germany](#) have also announced anti-trust investigations into Amazon, also over concerns that Amazon would favour third parties using Amazon's logistical services over third parties that use their own.

Concerns about the rise of large foreign e-commerce players also led to pushback beyond the EU. The Indian e-market remains nascent, but it is expected to rise from US\$38.5 billion in 2017 to [\\$200 billion in 2026](#). India is thus a country of interest to many foreign e-commerce companies such as Amazon and Flipkart, a dominant e-commerce company of which US firm Walmart acquired an 81 per cent controlling stake in 2018. Especially after Amazon abandoned the Chinese market, the Indian e-market grew in importance. To address [concerns](#) about predatory pricing and deep discounting by US big technology companies, the Indian government introduced new laws in 2018. [These laws](#) are centred around limiting the power of companies that were then dominating the Indian digital economy (Flipkart and Amazon) and protecting new domestic firms by [following China's playbook](#) of successfully nurturing domestic giants. The Indian government [considers](#) data to be a national asset, so it introduced new data localisation measures. India's relationship with the EU is complicated by Delhi's new data-protection proposal, which calls for data localisation, requiring companies to store all critical data within India. One of India's most influential businessmen, Mukesh Ambani, is strongly in favour of this move, [arguing](#) that India needs to act collectively against data colonisation. In a way, this resonates with the EU's [new digital strategy that advocates for data sovereignty](#) and a process of [digital decolonisation](#) to become less dependent on US and Chinese technology companies. Nevertheless, India's way of trying to achieve this goal is diametrically opposed to that of the EU, which strongly opposes data localisation.

Hence, while coming from different viewpoints, both the Indian and European pushbacks against large e-commerce companies are motivated by the (mis)use of data by businesses. Creating more synergies between perspectives and approaches may lead to increased global leverage by the two partners. After all, the European and Indian e-commerce markets are important battlegrounds for US and Chinese e-commerce companies, and a strong stance to push for shared values will protect domestic e-commerce companies from unfair foreign competition.

3.2 Platform economy

The emergence of e-commerce, daily e-services (such as Uber, Airbnb and Deliveroo) and digital payment services (discussed in section 3.3 below) are resulting in an online 'platform economy', wherein [big technology companies offer](#) a wide range of online structures with a relatively low number of employees. For example, [Uber](#) has just over 22,000 employees, while working with 3.9 million drivers who complete more than 14 million trips per day.

While many emphasise the opportunities of the platform economy, the disruptions to regulation, uneven power structure between platforms and their workers, and the responsibility of the ecosystem beyond the enterprise are in some ways [problematic, as they may ultimately undermine the regulatory power of a government, and thereby democracy as such](#). The platform economy changes ways of working, socialising, value creation and competition for profits. The [vast social and economic impact of online platforms](#) ranges from human health, polarisation and misinformation, to economic competitiveness, consumer privacy and public services. The EU is only slowly catching up with this reality – a reality that is complicated by the fact that US (and increasingly more Chinese) big technology companies (so-called Big Tech) have developed a strong presence on the European continent.

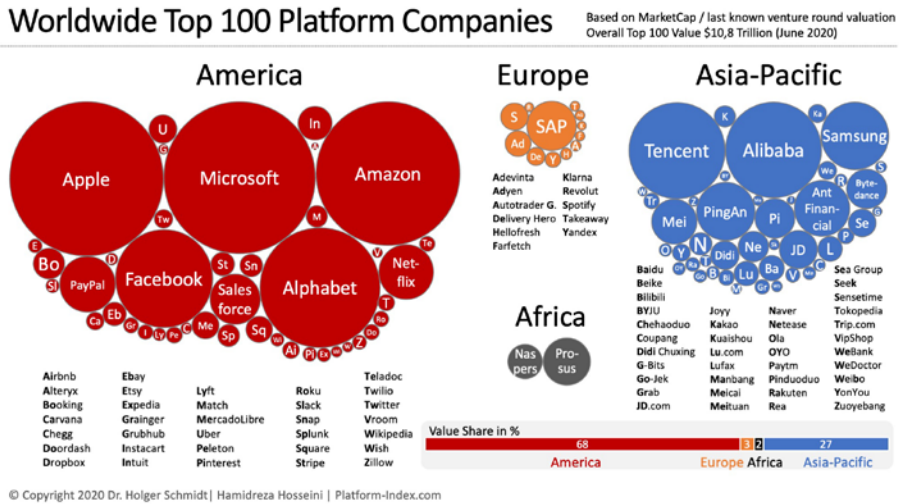
The traditional 'platforms' – that is, social media platforms – were once scattered among the EU member states, but increased globalisation and people-to-people exchanges resulted in a dominant position for Facebook and Twitter, at least in Western markets. National alternatives, such as [Tuenti](#) in Spain and Hyves in the Netherlands, have all been forced out of the markets or were bought by competitors once users started to switch to Facebook and Twitter.

The European Commission aims to [foster](#) a 'trusting, innovation-driven online platforms' environment in the EU', underpinned by a level playing field, responsible behaviour, transparency and non-discriminatory markets. To regulate platforms operating within the EU, the European Commission drafted the [Digital Services Act \(DSA\) package](#). This creates a legal framework for digital services based on clear responsibility and ex-ante rules covering large online platforms.

The European Commission is thus battling to limit the power of these companies, which have come to set the rules of the game, imposing their business standards on their users and competitors. It is acting against so-called Big Tech '[surveillance capitalism](#)' – the process of commodifying personal data with the core purpose of profit-making. At the same time, the EU several years ago started a process of '[digital decolonisation](#)' by nurturing European technology giants and protecting European data.

It is facing an uphill battle, as only 12 out of the [worldwide top 100 platform companies](#) are European and those together account for a mere three per cent of value share (see Figure 3).

Figure 3 Worldwide top 100 platform companies



Source: Dr. Holger Schmidt / Hamireza Hosseini, www.platform-index.com

Just a few days before the publication of the EU digital strategy in February 2020, an informal group of European companies and trade unions published a set of ‘[Platform Fairness Principles](#)’. These principles correspond with EU efforts to keep dominant digital platforms accountable and to ensure fair competition, transparency and data privacy. The DSA’s public consultation period ended in September 2020 and is one of the stepping stones towards European digital sovereignty.¹⁰ While limiting the power of digital giants has been lauded by the European public, [European technology nationalism](#) and the draft DSA have also been portrayed as the foundation of the European great firewall.

International efforts on e-commerce and platform regulation

Asian countries like Singapore, India and Japan have their own approaches to limit dependence on US and Chinese foreign companies. These provide valuable reference points for the EU and its member states as they reconsider [strategic autonomy in the digital age](#).

10 The complete control over stored and processed data and also the independent decision on who is permitted to have access to it.

Singapore has taken a unique path to protect local vendors and platforms by way of a strong digital industrial policy. In the digital economy, the first-mover advantage is crucial, as markets quickly become saturated and second or third movers are challenged to gain market share. Since 2017, the Singaporean government has started to develop in-house technical solutions and purchase services from technology start-ups rather than offering grants to support them, through its [Smart Nation Initiative](#). Government-owned initiatives include the Networked Trade Platform ([NTP](#)) that connects industries digitally; the Industry Transformation Maps ([ITMs](#)) programme that addresses issues within each industry and deepens partnerships of the government with firms, industries, trade associations and chambers; and the Financial Technology ([FinTech](#)) that innovates the financial sector. In doing so, the Singaporean government has successfully nurtured its own digital businesses before foreign companies were able to win over Singapore's market.

As noted above, the Indian e-commerce market, albeit still nascent, is expected to rise to [200 billion US dollars in 2026](#). This has triggered the attention of large global technology companies, [seeking to attract](#) new users for their e-services as well as to gather demographic data on online behaviour and spending habits. The United States' presence is mostly observable in Amazon's [30 per cent market share](#) in India and Walmart's majority stake in Flipkart. In addition, for several years China was able to develop a significant position in India. [Filling the gap](#) created by a lack of Indian venture investors, Chinese companies became investors to eighteen of 30 Indian 'unicorns'. While the Indian government publicly opposed China's Belt and Road Initiative, it was generally welcoming in the digital field. This began to change in 2019 when the [Indian government](#) started to adopt protectionist policies and foreign online retailers were restricted by, among other measures, demands to store data locally. This approach aimed to support Indian e-retailers and high tech companies at the expense of foreign competitors, as foreign companies would experience rising costs. Recently, amid the Sino-Indian border conflict, India has moved to [ban 59 Chinese apps](#), including the widely popular TikTok and WeChat apps. Differences notwithstanding, the EU and individual EU member states have an interest in broader and deeper engagement with India in the digital domain – to discuss openness, transparency and inclusiveness against a shared concern about growing Chinese influence.

Lastly, Japan has often been [overlooked](#) by companies searching for e-commerce opportunities. Nevertheless, its highly urbanised population and developed economy have been among the fastest-growing e-commerce markets globally. With excellent infrastructure and an internet penetration rate above 93 per cent, the EU may want to engage with Japan when exploring options to counter the influence of US and Chinese e-commerce companies and platforms. Aiming to nurture and retain (problem-solving) businesses, both the EU and Japan are devising policies to assist promising start-ups, also to avoid losing them to US or Chinese giants during the scaling-up. The EU and

Japan stand to benefit from [more engagement](#) with each other's strategic thoughts and best practices.

The EU's turn from defensive to offensive measures?

The main difference between Singapore and Japan on the one hand, and the EU on the other, has been the origin (key driver) and the approach of measures taken domestically. The EU has been primarily acting from a defensive standpoint, trying to regulate already established e-commerce companies and platforms, and thereby enforcing new rules in a game that started over a decade ago. Singapore and Japan, on the other hand, observed the growing influence of US and Chinese companies and acted upon this by nurturing and supporting national alternatives. India was a latecomer, but implemented strict regulations to limit the influence of foreign companies.

Moving forward, the EU and individual EU member states can explore Singapore's approach in their attempts to nurture and maintain European e-commerce companies and platforms, especially promising start-ups. While hiring engineers to develop further digital technologies within the government may be too far-reaching for most Europeans' liking, elements of Singapore's approach will prove valuable as the EU strives to strengthen its digital autonomy. Moreover, the EU might want to create a dialogue with India and other Asian partners concerning their experiences with US and Chinese influence (attempts), but also to discuss possibilities to join forces and create viable, reliable and transparent alternatives to US and Chinese companies.

3.3 Digital payments

As e-commerce, platforms and internet banking became more popular, e-payment systems also grew. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is the international organisation managing most international bank-to-bank payments, by way of the Business Identifier Code (BIC). In the last decade, various alternative systems known as '[digital wallets](#)' have entered the market, of which US-based PayPal is the most known in Europe. A digital wallet makes carrying an actual wallet obsolete, by facilitating customers' online payments.

Since 2018, Alipay has been [finding its way](#) into Europe, partnering with companies in Italy, Norway and the United Kingdom. [Over 50 countries](#) now accept Alipay, of which 29 are European and a handful are South Asian. Alipay's electronic payment platform also offers foreigners visiting China the option to download Alipay's [Tour Pass](#). This feature allows them to use Alipay as a prepaid card service to which money can be transferred, whereafter the app can be used to pay in Chinese shops. Alipay and WeChat Pay also faced global [controversy](#) during the COVID-19 pandemic because of the released QR code system that reads the smartphones and determines whether or not a

user poses a health risk. From a privacy perspective, this new feature caused concerns among policy-makers in Europe.

[Big Tech firms](#) including Google, Apple, Facebook and Amazon have successfully developed financial services during the last decade. While services of large technology companies such as Apple and Microsoft generally lack interoperability, the digital payment sector has a wide array of suppliers that are highly interoperable to transfer cash smoothly on a global level. Most e-commerce websites or digital services offer multiple payment options, [ranging](#) from Alipay and WeChat, to PayPal and direct payment systems through customers' own bank accounts by using, for example, Swish (in Sweden) and iDeal (in the Netherlands).

The financial sector may be an example for other digital services, such as operating systems, to become globally interoperable without losing their competitive advantage. Nevertheless, concerns remain about dominant companies forcing competition out of the market. China's top anti-trust agency is now looking into the possibility of [launching a probe](#) into Alipay and WeChat Pay for this matter in the Chinese market.

For Europe, it might be interesting to look beyond the now emerging financial payment methods to digital currencies (so-called 'cryptocurrency'). Bitcoins have been the first publicly known [cryptocurrency](#) and alternative digital currencies, using Blockchain and distributed digital ledgers, are now underway. Since 2014, more than 500 digital payment systems and currency companies have been [founded](#). Some are even considered as challenging financial systems at their core. Facebook's Blockchain-based digital currency Libra has permission to be developed and its [launch](#) is still planned for 2020. The Chinese government also started a pilot programme for an official [digital renminbi \(RMB\)](#), and it is expected that the currency will be used during the Beijing Winter Olympics of 2022.

EU member states need to step up their efforts in supporting their own new and upcoming initiatives. Private US or Chinese state-led initiatives are highly competitive in adopting and funding new initiatives. Singapore is able to out-compete the large scale of those initiatives, yet the EU and Japan, while ranking high on research and development, seriously lag behind in commercial adaptation of their research. In order to overcome this challenge, the EU and Japan can benefit from [more engagement](#) with each other's strategic thoughts and best practices in emerging digital fields. Digital payments may be the first new field that the EU and Japan can discuss.

A separate but clearly related subset that also deserves mention here is digital financial inclusion – efforts that may be labelled '[digital official development assistance \(ODA\)](#)'. India stands out as having clear potential in this field, largely thanks to its domestic experience with the use of digital tools to spur development. India has had remarkable success with its efforts to enhance digital financial inclusion through digital payment

systems, which raises the question of whether this success can be exported to other developing countries, either by India as a development player on its own, or in a trilateral format with European partners. Trilateral cooperation with Indian companies with a proven track record could facilitate improved access to countries, particularly in Africa. Cooperation may be sought with India's Centre for Digital Financial Inclusion (CDFI), which promotes the use of technology to support its welfare programmes and financial mainstreaming for the poor, with a valuable track record on digitising the delivery of benefits, from implementing data-driven frameworks from governance to farm services and promoting basic financial literacy using digital communication tools. For now, the CDFI operates only within India, but its experiences could be of benefit to individuals in many other developing countries.¹¹

3.4 The multilateral context: the WTO and OECD

The World Trade Organisation

The rulebook of the World Trade Organisation (WTO) was largely created before the internet revolution, leaving states dependent on a patchwork of bilateral regulation rules on e-commerce rather than a comprehensive global framework. To address this flaw, the WTO [in 1998](#) established an e-commerce initiative to connect international trade rules with digital trade, including e-commerce, goods, services and the transmission of information and data across borders. From 2001 to 2016, twelve so-called Dedicated Discussions have been held under the auspices of the General Council. Central to the discussions were effective ways to include less-developed countries and [concerns](#) about the digital gap, where developed economies are the main providers of digital services and developing countries are users of these services, further exacerbating global horizontal inequality.

It was only in 2019 that [76 WTO members](#) launched negotiations on the trade-related aspects of e-commerce. [The WTO aims to](#) create a multilateral legal framework that consumers and businesses can rely on to improve trust, tackle barriers, guarantee validity of e-contracts, ban customs duties on electronic transmissions and address forced data localisation requirements. The EU has been one of the initiators of this dialogue.

While the protection of customers and companies is gaining momentum, especially because of increased e-commerce and platform transactions during the COVID-19 pandemic lockdowns, the WTO is having a hard time [regaining](#) its credibility. The US blocking of the two new members of the WTO's Appellate Body has paralysed the

11 Author's interview with CDFI director Krishnan Dharmarajan on 17 January 2020, Bangalore.

WTO's ability to rule on new trade disputes between member countries since then. Additionally, the candidates now in the running to become the new WTO president cannot take a strong stance, as the [vital challenge](#) remains to keep the United States and China on board while simultaneously defending the logic of multilateralism. Nevertheless, the WTO may take on an influential role, as it is the only international organisation that can bring 164 countries together to discuss new e-commerce and digital platform regulations.

The Organisation for Economic Cooperation and Development

Another organisation focusing on the digital economy is the Organisation for Economic Cooperation and Development (OECD). During the 2016 Cancún Ministerial on the Digital Economy, OECD members [recognised](#) digitalisation as a catalyst for innovation, growth and social prosperity, and thus the need for a holistic and whole-of-society approach. In the OECD's 2019 report, in which the OECD [unpacks e-commerce](#), it identified gaps between older and younger e-commerce users, higher and lower levels of education, and also differences between rural and urban areas. These differences are often referred to as the 'digital divide', in a broader context than just e-commerce. In 2020, the OECD [addressed](#) a report to the G20 Digital Economy Task Force on how a common framework could be established.

Within the OECD, platforms and platform regulation are key topics under discussion in the digital domain. This includes rewriting tax rules to better regulate tax payments by [Big Tech companies](#), most of which are based in the United States. [About half of the European OECD member countries](#) moved ahead with new tax rules, with France being the first in Europe to introduce its own [digital tax](#). Italy, Hungary, Poland, the United Kingdom and Austria also [implemented](#) a Digital Services Tax. Spain, Belgium, the Czech Republic and Slovakia have also proposed concrete steps to implement a Digital Services Tax. The United States responded with [retaliatory threats](#), including trade tariffs. In July 2020, the OECD released its global tax-reporting framework: the Model Rules for Reporting by Platform Operators with respect to Sellers in the Sharing and Gig Economy ([MRDP](#)). This framework requires platforms to [report](#) to tax authorities the income they realised by offering accommodation, transport and personal services.

OECD members have already established a train of thought together on platform regulation, so a leadership role by the OECD in pushing for increased regulation appears to be appropriate. The main pitfall of the OECD becoming the lead organisation in shaping the framework of the platform economy is the [exclusion](#) of all African and most Asian countries, other than Japan and South Korea. After all, close cooperation with huge digital economies such as China, but also emerging (digital) economies in South-East Asia and Africa, is of paramount importance to create a global perspective, instead of a Western perspective, on the regulation of e-commerce.

4 Telecommunications infrastructure

Alongside the regulatory and business domains, telecommunications infrastructure is a key element in the current global battle for leadership in digital connectivity. Two subsets are highlighted here: 5G wireless network technology; and Cloud computing infrastructure (specifically GAIA-X, the European alternative-in-the-making to US and Chinese Cloud offerings). Smart cities could be considered a third subset under this category, but are detailed [elsewhere](#). They are, moreover, built on 5G infrastructure and interwoven with the business dimension, meaning that their full potential will be unleashed once 5G networks become deployed and commercialised. In the multilateral context, the International Telecommunication Union (ITU) is a key institution in this field, as the architecture of the internet is (re)designed there, with a Chinese proposal for a new internet protocol (New IP) presently on the table.

4.1 5G networks: the embodiment of US–China tech rivalry

The global rollout of 5G networks has become a defining element of US–China tech rivalry. Both the Chinese and [US governments](#) have gone to unusual lengths to persuade countries worldwide to side with them. From 2018, Washington embarked on an [aggressive diplomatic campaign](#) to convince others to refrain from using Chinese tech company Huawei’s equipment.

Digital infrastructure is the backbone of the modern digital economy. The accompanying ability to set rules and standards provides significant strategic advantages for countries’ economic and military capabilities. Throughout the post-Second World War period, the EU and US benefited greatly from their established positions, and in the present Fourth Industrial Revolution, China aims not only to strengthen its technical capabilities (and thereby its ability to withstand US sanctions), but also to [shape](#) standards and regulations. This is clear from its forthcoming ‘[China Standards 2035](#)’, which complements ‘Made in China 2025’, and is practised hand-in-hand with its globally operating Chinese tech firms.

Technical specifications underpin digital infrastructure, such as 5G networks, and translate into the standards that are most effective when [uniformly adopted](#) globally. The technical specifications are set by countries leading the technological innovation. In the 1990s, the United States [lost the 2G](#) competition to Europe, especially to Nokia and Ericsson, and [Japan took the lead](#) in 3G development and roll-out between 2000

and 2007. Through a [private-sector-led strategy](#), entailing huge investments and an increasing supply of spectrums, the US quickly gained 4G leadership. Since 2011, this has resulted in an entire [ecosphere](#) created by US companies, as smartphones and the world wide web became more advanced and integrated into society. Today, the United States seems to be missing out in the race for 5G dominance, with only two European companies, Nokia and Ericsson, South Korea's SKT-KT and LGU+, and Chinese firms Huawei and ZTE having the knowledge and equipment to roll out 5G networks.

The expertise and technical know-how of European and Chinese competitors are comparable. Therefore, companies' (political) strategies and tactics will determine which company 'wins' in the 5G market. Huawei is currently building on its strong base in 4G, trying to solidify its global presence in Europe, Africa and South-East Asia. Mainly thanks to support from the Chinese government, Huawei can offer extremely competitive prices in foreign markets; any global losses can be compensated with domestic profits, with Huawei and ZTE having more than 90 per cent market share in domestic Chinese 5G sales in 2019. Internationally, Chinese companies are facing difficulties, as concerns about cyber security and espionage are widespread – fuelled, at least in part, by the US. Appealing to its high-quality infrastructure and reliable image, Sweden's Ericsson has been able to use Huawei's issue with cyber security to its advantage. [Since 2019](#), Australia, New Zealand, Japan, Taiwan and the US have banned, or are phasing out, Huawei in their mobile networks, thereby automatically opting for the European alternatives for their 5G infrastructure.

European capitals take diverging approaches on this matter. The United Kingdom stands out for its explicit U-turn, [banning](#) Huawei completely in June 2020, in a dramatic reversal of its January 2020 decision, which gave Huawei [the green light](#) to assist building the UK's 5G network. Separately, the Dutch telecommunications provider [KPN](#) [stands out](#) as the only European-based company that has decided to switch completely to a Huawei network for offering 4G and 5G services to its customers.

Asia–Pacific: a region to watch

Like the EU, the Asia–Pacific region is also an [important locus for 5G competition](#). While advanced economies like Japan and Australia have already decided on their 5G strategies – effectively banning but studiously avoiding any mention of Huawei – many developing countries are still in a bind between their dependence on low-cost technology to advance their own economies and the potential national security risks.

In this respect, South Korea is also facing the [security-trade dilemma](#) concerning the 5G adaptation of Huawei, Nokia or Ericsson, and Seoul may be a surprisingly like-minded partner in the roll-out of 5G networks in Asia. South Korea has an ambitious 5G goal to cover the entire country by the end of 2022 with domestic 5G technologies

and products. SK Telecom and Ericsson have played a significant role in this as they provided the first commercialised 5G stand-alone network in [South Korea](#). In 2019, South Korean technology companies Samsung and LG also launched 5G-compatible smartphones, thereby integrating 5G technologies into the daily lives of South Korean citizens. LG has already set up a 6G research centre at the Korean Advanced Institute of Science and Technology (KAIST), and the Finnish University of Oulu, as well as Finnish tech giant Nokia, have started research into 6G possibilities.

For the EU, engaging with South Korea on telecommunications matters and the commercialisation of 5G may be opportune. In the private sector, EU–South Korean ties now exist, with the SK Telecom–Ericsson collaboration on stand-alone 5G networks in South Korea. By engaging both private and public actors in discussions, best practices can be shared, as well as experiences for the roll-out of a commercialised 5G network in Europe.

Additionally, the EU can go on the offensive on [6G](#) and see whether the EU, South Korea and Japan can coordinate their research efforts into next generation wireless communication technologies. The [EU–Japan Partnership on Sustainable Connectivity](#) and Quality Infrastructure could be a starting point for enhancing international cooperation, also in exporting 5G infrastructure into third regions including the Indo-Pacific, Africa and the Western Balkans. After all, the EU and Japan share similar concerns, and Japan is now trying to nurture Japanese providers, together with South Korean partners, into becoming key players in 6G. By pushing for a 6G network to be developed rapidly, a difficult choice between the United States and China [may be averted](#). Swift action is needed, however, as Beijing has also announced that China has launched research and development efforts [into 6G networks](#).

Japan and Singapore might also be interesting partners to cooperate with and share experiences balancing US–China pressure in the field of telecommunications. Japan and Singapore both banned Huawei successfully out of their markets, without experiencing negative repercussions from Beijing. Concerns over national security and trade underpinned the decision in Japan and Singapore, while this dilemma remains unanswered in many EU member states. Now, the technologically advanced Singapore and Japan are prioritising the implementation of 5G networks, a stage that various EU member states have also entered, but with the [disadvantage](#) of having vast EU member-state differences in internet coverage and 5G readiness. Therefore, engaging with Japan and South Korea – both on their considerations regarding the trade-offs between national security and trade, and on their experience in successfully implementing 5G networks – may contribute to EU policy-makers' knowledge.

Engaging with India on the implementation of 5G networks will be hard, but also the most valuable, as India's immense telecommunications infrastructure will be an important stepping stone in obtaining leadership in the telecommunications domain.

Through its [Digital Infrastructure: the backbone of the digital economy](#) report, the Indian government discusses its dependence on affordable digital communications infrastructure, but also the dilemma between national security and trade. Moving forward, the EU and its member states could partner with the United States in India to offer a secure, privately led and privacy-oriented alternative to China's competent and inexpensive bid. However, the partnership between the United States and EU is currently complicated by US threats of tariffs [against Brussels](#). To counter China's international technological dominance, the transatlantic relationship must be restored or reshaped, while the EU simultaneously needs to find like-minded partners.

4.2 Cloud computing

A new infrastructural element, encompassing the ITU's mandate and overlapping with data governance, is Cloud computing. [Ninety per cent](#) of the world's data has been created in the last two years, showing the vast growth and increase in digital innovation, and this data has to be stored somewhere. Cloud computing offers hardware, software, databases, storage and analysis on demand, thereby quickly replacing traditional computing – consisting of local corporate data centres, software and hardware updates. Cloud computing eliminates the costs of implementing and maintaining on-site data centres, increases the flexibility to scale up and act quickly on a global level, is always up to date and offers a wide array of low-cost options for data back-ups.

However, existing Cloud offerings are dominated by [US](#) (such as Microsoft, Amazon Web Services and Google) and [Chinese providers](#) (Alibaba, Tencent and Baidu), with significant market power and rapidly upscaling Cloud infrastructures. Cloud providers are legally subject to their home countries, thereby creating doubts about whether the data sovereignty of European companies and citizens can be guaranteed, especially since US Cloud companies' data on servers abroad must [be accessible to intelligence services](#) and Chinese Cloud services have the obligation to share any data with the Chinese intelligence services when demanded under the Cybersecurity Act.

While European alternatives have not offered any comparable market capitalisation, scalability or breadth of applications because of their activities in specialist niches, [22 firms](#) have been involved in the creation of a new Cloud computing initiative: [GAIA-X](#). This German–French private-sector initiative, initiated in 2018, unites European Cloud and Edge services, with the aim of providing a secure infrastructure for industrial data and cross-border movement of such data, while also regaining the digital sovereignty of European member states. Non-European partners are equally welcomed, but they have to comply with European data-protection rules. Currently, over [300 organisations](#) worldwide are dedicated to the project and the GAIA-X infrastructure is expected to be launched in late 2020 or early 2021.

In addition to upholding European digital values, GAIA-X is also an attempt to leverage the EU's regulatory power and to set a 'golden standard' for global data infrastructure, just like the GDPR, which is widely adopted globally as a standard for data protection. The Joint Declaration for a Cloud Federation that is to be adopted at the European Council in October 2020 will also contribute to this purpose. In synergy with the [European federation of Cloud infrastructures](#), the intention to launch a European Cloud services marketplace in 2022, and to establish a governance framework and an EU Cloud rulebook, shows that the European Commission is embarking on concrete, offensive action in this subset of digital connectivity.

For Europe, the creation of GAIA-X is timely, as many companies are now deciding which Cloud applications will be used as a foundation for their data and business models. In 2019, [only one in four businesses](#) are using Cloud computing for their daily operations in Europe, but many are expected to take up Cloud computing in the years to come. To prevent vendor lock-in, GAIA-X connects various infrastructures to [ease the movement](#) of data among Cloud providers. This will also support a level playing field for Cloud providers included in GAIA-X and offer a new side of Cloud computing to the existing, separate Cloud providers from the United States and China. To create more leverage for GAIA-X and create more interoperability between global Cloud services, the EU is starting with interesting 'adequate' countries, since these countries have comparable levels of data protection. These countries can thus easily be integrated into this initiative. Second, the EU can reach out to like-minded partners and show its competitive advantage over US and Chinese Cloud services, namely the interoperability between the Cloud services. In this way, countries do not have to choose one specific Cloud service and stick to this choice, and competition between Cloud services to offer the best amenities and solutions will be stimulated now and in the future, creating the best user experience.

4.3 The multilateral context: the ITU and beyond

[Beyond](#) the roll-out of 5G infrastructure, the global race for technological leadership also involves standards, rules and norms in other fields, such as the Internet Protocol. The EU and its member states have to engage more actively with Japan, South Korea and Singapore to defend their interests in the global arena. One multilateral organisation of particular relevance is [the International Telecommunication Union](#) (ITU), a UN agency that focuses on information and communication technologies (ICT) and discusses the development of technical standards to ensure interconnectedness between networks. While the ITU's regulation is non-binding and adopted voluntarily, the organisation does set precedents for the global adoption of ICT.

Since 2016, China has been increasingly active in the ITU. This is [evident](#) from the rising numbers of Chinese employees working at the ITU. In 2018, Chinese experts held 36 [leaderships](#) in the study groups of the ITU-T (the Telecommunication Standardisation Sector of the ITU) and the Asia-Pacific Telecommunication Standardisation Forum, and 77 served as (associated) [rapporteurs](#). China is also visible in the growing [number of contributions](#) submitted, especially since 2009 with more than 900 contributions being made annually. This [volume of contributions](#) creates an image of China having the dominant view in various ITU-related discussions, for example on [surveillance technology](#) or, more specifically, in the discussions of surveillance of people within cities. Moreover, the Chinese government – and Chinese companies, which may join meetings to give technical input – has been committed to its *New Internet Protocol* to reshape the worldwide web through the ITU. States acknowledge that today's [model of internet governance](#), entailing lawless self-regulation by private, mostly American companies, is suboptimal and should be changed to meet the needs of the future. They are, however, also concerned that the *New Internet Protocol* is not (yet) ready to replace the existing IP-identification system, as it might spur governments' control over the internet or cause a 'splinternet' with various systems operating in parallel.

EU member states, but not the EU itself, are members of the ITU. The EU does, however, coordinate EU member states' responses to proposals discussed in the ITU working groups. So far, the United States and the EU have been acting defensively, largely reacting to proposals of other countries, especially China. This creates a situation in which China is [setting the tone](#) of the debate, while the EU is pushed on the defensive in protecting a free and open internet, without advocating for its own suggestions.

Clearly, the EU and its member states also need to act more assertively and become more active in submitting proposals in internet governance bodies such as the ITU that align with the EU's digital strategy. This is a crucial step to further a democratic decision-making process rather than a process that is dominated by a few large players. European proposals will offer an alternative to the Chinese proposals – as well as the current internet design, which largely benefits US Big Tech – and illustrate the appeal the 'third way' of Europe. First steps in this direction are already being made, by way of the [Next Generation Internet \(NGI\) initiative](#), which is dedicated to 'fostering a vibrant Open Internet movement that links research, policy and society for the benefit of society'. On this front, the EU stands to benefit from further cooperation with like-minded countries such as South Korea, Japan and Singapore, whose support will be needed to succeed with implementing this [vision to reshape the internet](#).

Beyond the ITU, digital connectivity is also discussed in the G7 and G20 contexts, for example in the [G20 Digital Economy Ministers Meeting of 2020](#). Joint statements recognise universal, secure and affordable connectivity as an enabler of development and a catalyst for inclusive growth and sustainable development. Indeed, the

development track may be the most important for the G20, as it works to further sustainable infrastructure development, including in the digital field.

As knowledge partners, the OECD and ITU take part in the discussions that encompass, but are not limited to, trustworthy AI, Data Free Flow with Trust, Smart Cities, measurements of the digital economy and security in the digital economy. In 2019, the [G7 digital technology ministers](#) also invited UNESCO, as well as the four major non-G7 democracies (along with the OECD and ITU), to discuss the digital transformation in AI, platforms and data-based infrastructures. Even if discussions still appear rather superficial and statements generic, the G20 may be the only forum with global participation where limited convergence is taking shape on the issue.

5 Conclusion

Technology and digitalisation are at the heart of the hardening Sino-American conflict. While China has established itself as a science and technology powerhouse, the United States is trying to maintain its economic competitiveness and supremacy in emerging technologies. The EU is now having to develop its own way next to the superpowers – disagreeing with the US zero-sum mentality and objective to curb China’s technological rise, but simultaneously having clear concerns about its global competitiveness *vis-à-vis* China, as well as the ‘Chinese characteristics’ that China’s growing global tech presence is having on norms and standards in this field. At present, the EU and its member states are largely playing on the defensive, shown by the adoption of new industrial policies, including on investment monitoring and export controls. These policies are mainly a response to existing developments in China and the perceived lack of movement on some long-standing European requests, such as reciprocity on market access and the free and open internet.

The COVID-19 pandemic has accelerated global digitalisation and added further urgency for the EU to act on the challenges in this field. Regulation, business and infrastructure are central to this discussion, and this report has elaborated upon every field to explore possible cooperation with like-minded Asian countries. The table below shows a brief summary of our findings.

Figure 4 Potential for cooperation by European countries with selected like-minded partners

Country	Regulation		Business			Infrastructure	
	Personal data flows	Non-personal data flows	E-commerce	Platform economy	Digital payments	5G networks	Cloud computing
India	X	X	V	V	V	V	tbd
Japan	V	V	n/a	V	V	V	V
Singapore	X	V	V	V	n/a	V	tbd
South Korea	V	V	n/a	n/a	V	V	tbd
United States	X	V	X	X	n/a	V	tbd

V = potential for further dialogue and cooperation in this field

X = conflict of interest and/or approach in this domain

tbd = to be discussed, i.e. international discussion on a topic is yet to be initiated with a specific country and/or the position of a country is unknown in this specific field

n/a = not available, i.e. assessment cannot be made based on the findings in this report.

Transatlantic cooperation has been the natural reflex of the EU and its member states in the post-war period. Also in the Fourth Industrial Revolution, cooperation with the United States remains crucial. That said, while the EU shares most of Washington's concerns about China as a new technological power, it does not wish to use security and normative concerns as an excuse to curb China's growing economic influence. Instead, the US and EU should cooperate to uphold their economic competitiveness *vis-à-vis* China, on technology, standards and norms in the digital field. However, cooperation is complicated further by the fact that certain US tech companies' practices run counter to Europe's 'human-centred' approach, which emphasises online transparency, privacy and digital inclusiveness. Strikingly, deeper and broader cooperation with the US will therefore depend on a greater independence of the EU from those companies in the long term, combined with EU competence to act on behalf of its member states in these fields.

Data regulation and the view on data privacy will be an indicator of how countries balance individual, business and state interests. Having a similar human-centred focus, Japan and South Korea are natural 'adequate' partners to enhance practical cooperation, also in fields beyond data, such as e-commerce, 5G networks and Cloud computing. Japan and South Korea are also strong allies in maintaining and supporting the international rule-based system. Aligning international efforts in international organisations to advocate for a human-centred approach will thus likely be beneficial. The geographical closeness of Japan and South Korea to China has led to greater dependence on and intertwinement of those countries with China. When cooperating, the EU could learn from the more cautious but effective approach of Japan and South Korea, especially as these countries are used to dealing with China's growing influence in the region.

Singapore is actively trying to engage the EU concerning digital trade, and is most valuable as a partner in e-commerce and the platform economy. Currently, however, Singapore is getting little response from EU member states on this subject. It seems that member states first want to determine their stance within the EU framework before entering into dialogue with third countries. To create awareness, the EU might want to support dialogue, even if countries do not yet have a clear national stance. The exchange of ideas and thoughts will already be valuable for best practice learning and (re)positioning.

India is experiencing many challenges that resemble those of the EU when it comes to e-commerce and the platform economy. Large US and Chinese platforms have gained ground and force traditional and national e-commerce companies out of the market. More and regular meetings between government officials, experts and representatives of businesses and banks in so-called track 1.5 dialogue settings, combined with joint research, will be beneficial to learn from each other's challenges and approaches. With regard to data, India's concerns – in particular regarding the influence of the big

technology companies – resemble those of the EU. However, the Indian government's approach to implementing data localisation provisions contradicts with European norms on data regulation and data localisation. On e-payments, India may be a strong partner. And the Indian government has developed great know-how and practice concerning digital financial inclusion, albeit so far mostly in the domestic context. Moving forward, it seems opportune to connect Indian expertise on digital financial inclusion with larger questions on e-commerce and data regulation, as a way to further the debate.

An anomalous category is Cloud computing, where large American and Chinese Cloud providers are at present 'hyper-scalers' – that is, companies that not only dominate the public Cloud and Cloud service industries, but are also active in numerous related domains, such as e-commerce and e-payments. The EU and its member states are still finding their way in designing and kick-starting GAIA-X. This new initiative can be understood as a platform that connects Cloud-hosting services rather than being a Cloud service provider itself. What makes GAIA-X unique is the fact that Europe's strict data-processing rules underpin the platform, which does not exclude foreign companies but rather aims to convince those companies to adhere to the same strict rules. Considering Japan's adequacy status, Japanese companies are natural partners to be included. However, to boost Europe's influence in the field, as well as its human-centred digital approach, getting Amazon or Alibaba on board would be an important step forward.

Slowly but steadily, the EU is claiming its space in the digitalised world. GAIA-X demonstrates that European actors are going on the offensive, creating a strong and sustainable Cloud infrastructure that unites small European initiatives and provides an alternative to American and Chinese Cloud providers. Alongside such 'EU-only' initiatives, working closely together with like-minded Asian partners will benefit the EU and its member states as they seek to fine-tune and implement their digital strategies – at home, in third countries, and in international networks and institutions.

Annexe 1

Subject	GDPR	China Cyber-security Law	South Korean PIPA	US Data Regulations	Indian Personal Data Protection Bill	Japan Act on the Protection of Personal Information	Singapore
Applicability	1. To legal persons (businesses, governments and other registered organisations)	1. To all personal information controllers (legal persons established in China, businesses, governments, and other registered organisations)	All data processors, regardless of whether public or private	Not applicable. The US has no comprehensive privacy regulation, but there are regulations on sectoral privacy (e.g. HIPAA on personal health care data, CPNI on telephone data)	To all data processors	To all data processors	Organisations
Extraterritoriality	Yes	No	No	Not applicable	Yes	No	No
Explicit Consent	Yes	Not always	Yes, consent is also required for anonymised data	No. Explicit consent as exceptions	Not always (only sensitive personal data such as passwords and health data require consent)	Yes	Explicit, even if the data are processed in anonymity

Subject	GDPR	China Cyber-security Law	South Korean PIPA	US Data Regulations	Indian Personal Data Protection Bill	Japan Act on the Protection of Personal Information	Singapore
Cross-border data flow	In principle denied. Data free flow with trust, with countries that have adequacy decision or the US for commercial purposes under the EU-US Privacy Shield ¹²	In principle denied, to allow for ad-hoc security assessment, reviewed by provincial level internet authorities	In principle denied, to allow for a data-protection agreement between transfer and receiver. Extra consent from individual required. Korean Land Act forbids, in any case, the export of map information	In principle always allowed.	Denied. Data localisation requirement for all 'critical personal data'. Other personal data should at least have one copy to be stored in India. Data localisation requirement does not apply to anonymised data	In principle denied. Data free flow with trust with countries that have the adequacy decision or with the data subject's consent	Internet Surfing Separation Policy stipulates that all public sector data should be localised. Personal data cross-border transfer in principle is denied, unless (1) the data processor will still control the data after the transfer, and (2) the target country offers comparable protection, or (3) the organisation has acquired specific consent from the data subject
Independent Enforcement?	Yes	No	No	Not applicable	No	Yes	No

12 In mid-July 2020, the European Court of Justice [invalidated](#) the Privacy Shield. See section 2.1 for further details.

List of abbreviations

AI	Artificial intelligence
APEC	Asia–Pacific Economic Cooperation
ASEAN	Association of South-East Asian Nations
BAT	(Chinese big technology firms) Baidu, Alibaba and Tencent
BIC	Business Identifier Code
CBPR	Cross-Border Privacy Rules
CDFI	(India’s) Centre for Digital Financial Inclusion
DCCP	Digital Connectivity and Cybersecurity Partnership
DDFT	Data Free Flow with Trust
DSA	(EU) Digital Services Act
DSR	Digital Silk Road
EU	European Union
FFD	Free flow of data
FinTech	Financial Technology
GAFAM	(US big technology firms) Google, Apple, Facebook, Amazon and Microsoft
GATS	General Agreement on Trade in Services
GDPR	General Data Protection Regulation
ICT	Information and communication technologies
IP	Internet Protocol
ITM	(Singapore’s) Industry Transformation Maps
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardisation Sector
KAIST	Korean Advanced Institute of Science and Technology
MFF	Multiannual Financial Framework
MFN	Most-Favoured Nation
MRDP	Model Rules for Reporting by Platform Operators with respect to Sellers in the Sharing and Gig Economy
NGI	Next Generation Internet
NTP	(Singapore’s) Networked Trade Platform
ODA	Official development assistance
OECD	Organisation for Economic Cooperation and Development
PPC	Personal Information Protection Commission
R&D	Research and development
SWIFT	Society for Worldwide Interbank Financial Telecommunication
UK	United Kingdom
US	United States
USMCA	United States–Mexico–Canada Agreement
WTO	World Trade Organisation