Ref. Ares(2020)4052088 - 31/07/2020

trigger
Trends In Global Governance and Europe's Role

D4.5 Explorative scenarios of governance by and of emerging technologies with far- reaching consequences on society and the economy

WP4 Governance and technologies: interrelations and opportunities

Grant Agreement n° 822735, Research and Innovation Action

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement nº 822735. This document reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.

TRIGGER

TRends in Global Governance and Europe's Role

Deliverable number:	
Deliverable name:	D4.5 Explorative scenarios of governance by and of emerging technologies with far- reaching consequences on society and the economy
WP / WP number:	WP4 Governance and technologies: interrelations and opportunities
Delivery due date:	31.07.20
Actual date of submission:	31.07.20
Dissemination level:	Public
Lead beneficiary:	CEPS
Contributor(s):	Andrea Renda

Changes with respect to the DoA

-

Dissemination and uptake

Public

Evidence of accomplishment

Report

Table of Contents

List of Figures

Principles and Guidelines for an overarching EU Governance Framework for Digital Technologies

TRIGGER Working paper – deliverable D4.5

Andrea Renda, 31 July 2020

Often defined as "unfinished business", the European Union's market integration process appears to have become more fragile than ever at the beginning of the new decade. Already in 2010, the Monti report denounced the existence of a Single Market "fatigue", which made it difficult to complete the market integration process, especially in most difficult areas such as services.[1] Today, Brexit potentially threatens the future attractiveness of the Single Market, by depriving the Union of its third largest economy and leading to an unprecedented thorn in the EU's pride, as a Member of the Union sets sail. At the same time, the post-Brexit single market may become more cohesive and ambitious, as one of the most reluctant Member States leaves the group: the Union may also have the opportunity to re-discover some of the features of continental Europe's legal and economic traditions, from Civil Law rules to state-led industrial policy, which faced obstacles when the UK was in the Union.[2]

Against this background, the challenges for the Single Market project do not end with Brexit. To the contrary, EU policymakers are confronted with a frustrating prospect: as they try to complete the Single Market, technological evolution is pushing the frontier of integration further, requiring new efforts and policies to fully achieve the desired goal. In particular, the digital transformation is changing the traditional, textbook economics of market integration, based on tenets such as economies of scale and the four freedoms. The rise of the digital economy requires a radical change in the policies for the Single Market, as well as in the trade policies that underpin the whole market integration process. Trends such as the virtualisation, servitisation and platformisation of the economy (as described below), coupled with the rise of the Internet of Things and Artificial Intelligence, make market integration at once more appealing and increasingly challenging for EU policymakers, projecting the Single Market into a complete new dimension, in which the "Fifth Freedom" (the free circulation of non-personal data) is intertwined with new concerns with the need to protect fundamental rights, and at the same time secure Europe's technological sovereignty.

As EU institutions were struggling to complete the ambitious Digital Single Market strategy formulated by the Juncker Commission, technology has changed so fast that brand new policy initiatives are needed: the

[1] See "A new strategy for the Single Market. At the service of Europe's economy and society". Report to the President of the European Commission José Manuel Barroso, by Mario Monti. 9 May 2010

[2] D Kalff and A Renda, *Hidden Treasures. Mapping Europe's Sources of Competitiveness Advantage in Doing Business*. CEPS Monograph: Brussels, 2019. And A Bradford, *The Brussels Effect. How the European Union Rules the World*. Oxford University Press, March 2020.

Von der Leyen Commission seems to have marked a significant change towards a more assertive and future-oriented approach to digital policy. The new pillars of the Single Market 2.0 are not focused anymore on platform regulation, data protection and the free flow of non-personal data; while these remain very important pillars, the future of the Single Market will require that the whole internal market is seen as a layered ecosystem, in which infrastructure, rules, protocols and standards become a platform for large and small companies to develop value added solutions to the benefit of all European consumers. This "EaaP" ("Europe as a Platform") approach may also induce a change of terminology: what used to be mutual recognition will now mostly be related to interoperability; what used to be subsidiarity is translated into a choice between centralised, distributed and decentralised governance; open interconnection becomes "open API", and is applied far beyond network industries; and the free circulation of people is enhanced with a strong digital identity and verification layer. Importantly, especially after the appointment of Commissioner Thierry Breton, the Single Market 2.0 is becoming the *locus* of data spaces and ecosystems as the basic pillars of the future EU "competitive sustainability" agenda.

To be sure, achieving the Single Market 2.0 requires strong political commitment and will not prove easy, if the foundations of economic integration will remain as fragile as they are today. The COVID-19 pandemic has shown very clearly the difficulty of keeping the EU's "crown jewel" alive in times of despair and shortage of essential goods, such as medical protective equipment. The deterioration of the rule of law in some of the Member States (e.g. Poland, Hungary), the suspension of Schengen, the overall lack of solidarity between Member States and the temptation to use digital technology (*e.g.*, in the form of contact-tracing apps) in a way that jeopardises fundamental rights, are only a few examples of a more general crisis of the European integration project, which the von der Leyen Commission has barely managed to contain. At the same time, the COVID-19 pandemic is also accelerating the digital transformation, with the online economy becoming paramount for economic and social relations: this, in turn, makes the development of rules and standard for a trustworthy Single Market even more urgent.[3]

Can code succeed where law and politics have so far partly failed? In the remainder of this chapter, I outline the possible contours of a "Single Market 2.0". Section 1 below describes the current and the upcoming waves of digital transformation as featuring very different economic paradigms and consequences for EU policy. Section 2 discusses the reconfiguration of the Single Market as a layered ecosystem and describe the current Digital Single Market Strategy and the upcoming initiatives outlined by the European Commission, and partly affected by the COVID-19 pandemic. Section 3 provides a layered architecture for the Single Market 2.0 and outlines possible further avenues to speed up reform in a way that is consistent with all the cornerstones of the EU strategy for growth and sustainable development. Section 4 discusses the

[3] See Communication from the Commission to the European Parliament, the European Council, the Council, the European Central Bank, the European Investment Bank and The Eurogroup, "Coordinated Economic Response To The Covid-19 Outbreak", COM(2020)112 final, 13 March 2020.

consequences for EU actorness and effectiveness in the digital economy, and discusses possible EU policy options in the mid- to long-term. Section 5 briefly concludes.

1. Two waves of Internet evolution

Information technology (IT) experts traditionally approach architectural problems through modular structures, by distinguishing different layers and components of complex system goods and working through different options as regards on their interoperability.[4] Different choices in this respect lead to more closed architectures (e.g. the early Apple Macintosh), or more open architectures, in which different layers and components can be produced according to standard specifications by more than one firm (e.g. the early Microsoft Windows). The history of IT also suggests that no governance architecture is fully open, and typically one or more layers become dominated by one or a few players due to the emergence of network externalities, which lead to "winner-take-all" effects and often highly concentrated market structures at some of the layers.[5]

The Internet is itself depicted as a complex layered architecture, based on a massive physical layer, encompassing fixed and wireless communications systems, submarine cables and satellite systems, massive Internet Exchanges and data centres. The Internet age constituted a major enhancement of the original layered architecture of the personal computer, with the introduction of global-scale networking possibilities between computers and similar devices at the physical layer, and the definition of open protocols and standards that defined the traffic rules for data at the so-called "logical layer". Open standards such as the Internet Protocol and the File Transfer Protocol defined the characteristics of the Internet as a means of communication: as observed already in the 1990s by Lawrence Lessig, in a digital environment, "code, not law, defines what's possible".[6] In the case of the early Internet, the openness and neutrality of the standards defined at the logical layer determined the rise of the Internet as a formidable means of communication between peers, and a vehicle for permissionless innovation, in which at once users could preserve their anonymity ("nobody knows you are a dog", as in Peter Steiner's fortunate New Yorker cartoon in 1993); and developers could work on their applications without having to seek anyone's permission to reach the marketplace.

---

[4] See RN Langlois, "Modularity in technology and organization". *Journal of Economic Behavior & Organization* 49, 19–37, 2002; RN Langlois and P Robertson, "Networks and innovation in a modular system: lessons from the microcomputer and stereo component industries", *Research Policy* 21 (4), 297–313, 1992. See also H Chesbrough (2004) Towards a dynamics of modularity: a cyclical model of technical advance. In: A Prencipe, M Hobday (eds) The business of systems integration. Oxford University Press, Oxford, pp. 174–1-98; and H Chesbrough (2003) Open Innovation. Free Press, New York.

[5] C Shapiro and H Varian, Information Rules. A Strategic Guide to the Network Economy. Harvard Business School Press. Boston, Massachusetts, 1999.

[6] L Lessig (1999), Code and other Laws of Cyberspace, Basic Books.

That said, the Internet exacerbated the features of the original layered architecture of the personal computer: the introduction of a new layer, with an end-to[7]-end architecture and a growing ability to support data flows, generated an explosion in the amount of data available to end users, which in turn converted into a "poverty of attention".[8] The firms that managed to capture a significant share of that scarce resource (user attention), ended up becoming trillion-dollar corporations, or (as they are sometimes called in the economics literature) "superstar firms". Accordingly, the rise of the digital, interconnected economy has also coincided with a rapid, necessary transformation of the ecosystem dynamics, which would soon come back to haunt the early creators of the Internet, facing them with a rising market concentration, a declining neutrality, and gradual attempts to depart from the original end-to-end design.[9] This is what I call the "first wave of transformation" of the Internet.

1.1. The first transformation of the Internet: virtualisation, servitisation and platformisation

During the past two decades, the Internet has undergone a swift transformation, which led to the emergence of a more diverse layered architecture, and very peculiar forms of governance that hardly existed in the "brick and mortar" world. Understanding them is useful to identify the direction taken by the EU institutions in trying to reap the benefits of the digital ecosystem, at the same time minimising its associated risks.

First, the emergence of an end-to-end infrastructure, fuelled by growing computing capacity, high capacity networks and wireless connectivity, grandly expanded the possibilities of the digital economy to permeate the economy. The emergence of cloud computing made it possible for small companies to avoid buying or leasing hardware and downloading software and applications: these traditional transactions were replaced by "everything as a service", which led to enormous advantages both for individuals and businesses. The transition towards a "cloud era" allowed personal devices to become increasingly agile, while users were able to access hardware and software located in the cloud, as well as retrieve their files from cyberspace. Put more simply, a limitless "office LAN" where the main server was not located downstairs, but potentially on the other side of the globe[10]. This was the realisation of the so-called "age of access" already evoked by scholars in

[7] D Autor, D Dorn, LF Katz, C Patterson and J Van Reene. "The Fall of the Labor Share and the Rise of Superstar Firms*," The Quarterly Journal of Economics, vol 135(2), pages 645-709, 2020.

[8] Simon, H. A. (1971), Designing Organizations for an Information-Rich World. In Martin Greenberger, Computers, *Communication, and the Public Interest, Baltimore*. MD: The Johns Hopkins Press. pp. 40–41.

[9] MA Lemley and L Lessig, "The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era". UCLA Law Review, Vol. 48, p. 925, 2001. A Renda, Competition, Neutrality and Diversity in the Cloud, Communications & Strategies, No. 85, 1st Quarter 2012, pp. 23-44, 2012; A Renda, "Net Neutrality and Mandatory Network-Sharing: How to disconnect the continent", CEPS Policy Briefs, 18 December 2013; and A Renda, *Antitrust, regulation and the "neutrality trap"*, CEPS Special Report n. 104, April 2015.

[10] Cloud computing is a general-purpose technology of the IT field which became widely available in the late 2000. Vaquero *et al.* (2009) define it as "a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized Service Level Agreements". See L Vaquero, L Rodero-Merino, J Caceres & M Lindner, A Break in the Clouds: Towards a Cloud Definition. Computer Communication Review 39, 50-55, 2009. Cloud architectures are conceived to be very simple for end users but feature a very complex architecture "behind the curtains". As an example, Apple's iCloud

the 1990s. An age in which products and services are dematerialised to an extent that ownership and property rights become less important, and access rights become gradually more dominant[11]. The progress observed in ubiquitous connectivity and in compression techniques, coupled with enhanced possibilities to capture end users' attention, has gradually led to the emergence of access-based services. These include a variety of new business models, from pure streaming-based content access services (Netflix, Spotify) to intermediate forms (Apple Music + iTunes + Apple TV) which contemplate both ownership and access; and the so-called "sharing economy", based on a combination of network effects, granularity, and reputational effects (e.g. Airbnb, Uber). Many of these services rely on the "cloud" as a key resource for virtual access and use of IT resources.[12]

Thanks to the end-to-end nature of the Internet, the digitisation of information and ever-increasing capacity and connectivity, many parts of the economy have gradually transitioned towards virtualisation and servitisation, two intertwined phenomena that made the economy more agile, but also came with a price to pay in terms of inequality.[13] The "uberisation" of many sectors such as passenger transport, accommodation, child care, handyman jobs, IT work (e.g. Mechanical Turk, Upwork) and low-skilled jobs and many other markets has led to extreme situations in which humans, themselves, are offered "as a service".[14]

The end-to-end, digitised nature of the Internet also determined the rise of peer-to-peer interaction in various forms. The transition towards an access-based economy initially affected audiovisual content, creating significant disruption (first with peer-to-peer file-sharing, later with streaming-based services that almost restore the industry's profitability). Later, the rise of the collaborative economy reached unprecedented levels: in 2019 Bank of America Merrill Lynch valued the worldwide sharing economy at USD250b and further estimated that USD6 trillion in commerce could be disrupted by the sharing economy across sectors such as transportation, travel, food, retail and the media. This, representing approximately 8% of global GDP, is supported i.a. by the fact that eight of the world's 10 largest start-ups based on valuation are in fact sharing

---

allows the syncing of various devices with the cloud, such that the end user always enters the same environment regardless of the device used to connect to the network. Similar strategies have been pursued for the end user market by Google (Android), Microsoft (Azure) and Amazon (AWS). The most widely acknowledged taxonomies of cloud computing are those that relate to the basic cloud "modes" (i.e. Public, Private, Hybrid); and the main cloud "types" (i.e. Saas, AaaS, IaaS, PaaS). The provision of platform as a service (PaaS), for example, leaves more control of the configuration to the client that mere application as a service (AaaS) or software as a service (SaaS) modes. At the same time, private clouds are certainly more customized to the client's needs than hybrid or public clouds, which however enjoy clear economies of scale.

[11] See i.a. RW Gomulkiewicz, "The License Is the Product: Comments on the Promise of Article 2B for Software and Information Licensing", *Berkeley Tech. L. J.*, Vol. 13, Issue 3, p. 891, 1998.

[12] A specific case is 3D printing, which leads to a de-materialisation of the product, but rather than its remote access, entails a remote re-production of the product. This changes the role of the players active in the production cycle: in 3D printing, the borderline between manufacture and service provision is blurred due to uncertainty as to who should be assumed to be the manufacturer of the product, particularly when a 3D printer has been used somewhere in the value chain.

[13] The servitization (or "servicification") of the economy is a well-known process that largely pre-dates the Internet era. Hojnik (2016) reminds that the de-industrialization of developed economies started in the 1950s and the value added by manufacturing as a percentage of GDP is now below 15% in most OECD countries, and that "economic studies show that servitization is one of the economic megatrends of modern society, along with globalization, encompassing a broad range of business models that are currently occurring on the market"

[14] See J. Prassl, *Humans as a Service. The Promise and Perils of Work in the Gig Economy*, Oxford University Press, 2018.

economy businesses. And is likely to be further exacerbated by the impact of the COVID-19 pandemic, which led to an explosion in the demand for online services.

The proliferation of information sources and the need to store and retrieve data for a multitude of user transactions also led to the rise of a fierce competition for user attention (so-called "competition for eyeballs"). The explosion of Internet traffic in the 1990s and 2000s, powered by parallel streams of evolving technologies (data storage, broadband communications, data compression, innovation in traffic management) led to an emerging need for solutions that would reduce complexity: this solution was spontaneously developed by market forces, and mostly took the form of industry convergence towards a limited number of de facto industry standards at the higher layers of the architecture.[15] Today, the digital ecosystem has evolved into a much more diverse environment: the original open internet architecture co-exists with various multi-sided platforms, which coordinate, steer and manage the innovation taking place at the higher layer of the Internet architecture. This phenomenon, often called "platformisation", bears far-reaching consequences for innovation, competition and public policy.[16]

While a full review of the impact of platformisation on public policy would go beyond the scope of this chapter, it is worth looking at the peculiar governance features of platforms, as well as their impact on value distribution in the digital economy. A close look suggests that they are different from the traditional corporations. They are, indeed, a hybrid between the firm and the market, compared to the traditional distinction made in social sciences.[17] So-called multi-sided platforms are hierarchical structures serving various categories of users, in which most of the traditional activities of a firm are outsourced, automated, or "heteromated" (automated through the help of third parties).[18] A good example is Uber, a ride-hailing platform that matches independent contractors (drivers) with end users (passengers), in which the management and control of the former is largely done through a combination of algorithms and user reviews. The corporate structure and size of the firm in terms of factors of production (capital and labour) is extremely small compared to the amount of transactions that the platform generates and profits from. For example, Uber has approximately 20,000 employees, but "employs" more than four million drivers.

[15] Examples of de facto ICT industry standards in the pre-Internet age include Lotus 123, WordPerfect and other applications based on the original IBM PC architecture and the MS-DOS. Later, Windows 3.1 and Windows 95 (which ushered the Internet age) became widely diffused de facto industry standards. The case of Microsoft Windows is perhaps the most telling in the evolution that the ICT went through during the 1990s: the modular architecture of the personal computer entailed the existence of one layer (at the time, the OS layer), which would end up being essential in terms of connecting hardware with software and determining the compatibility and interoperability requirements of the whole system.

[16] See A Gawer, Platforms, Markets and Innovation, Edward Elgar, Cheltenham, UK, 2009.

[17] See RH Coase, *"The Nature of the Firm"*, Economica, New Series, Vol. 4, No. 16 November, pp. 386-405, 1937. OE Williamson, *The Economic Institutions of Capitalism*, New York: The Free Press, 1985. OE Williamson, "Public and Private Bureaucracies: A Transaction Cost Economics Perspective", Journal of Law, Economics, & Organization, Vol. 15, No. 1, JLEO Bureaucracy Conference, April 1999, pp. 306-342. And OE Williamson, "Transaction-Cost Economics: The Governance of Contractual Relations", The Journal of Law & Economics, Vol. 22, No. 2, October 1979, pp. 233-261.

[18] HR Ekbia and BA Nardi, *Heteromation, and Other Stories of Computing and Capitalism*,MIT Press, 2017.

The peculiar structure of platforms, their relatively small size, and the powerful network externalities that sustain their competitive position in the market contribute to strengthening their bargaining power vis à vis all categories of users. Such stronger market power increasingly contrasted with a regulatory approach that largely left these powerful intermediaries untouched, as a legacy of the early days of the "neutral" internet. The platformisation of the Internet had little to do with the early vision of a neutral, end-to-end "network of networks", open to all for permissionless innovation. Rather, it led to the rise of new gatekeepers, which occupy an almost unattackable position and continue to reap a large share of the value associated with the transactions they not-so-neutrally orchestrate. Not surprisingly, the need to govern the humongous amount of data their ecosystems generate also led these companies to increasingly invest gigantic sums in data-hungry machine learning systems, which came to dominate the digital environment as well as the AI landscape. From Netflix's recommendation system to Google's search engine, enormous investment has reinforced and ringfenced the market positioning of these platforms, enabling them to personalise product offerings, prices and conditions to an extent that no competitor could even come close to attaining.

Virtualisation, servitisation and platformisation have been extremely important drivers of change of the Internet ecosystem in the past two decades and have led to a massive change in the economy, largely consisting in a re-intermediation, rather than a dis-intermediation, of previous market transactions. Where the new business models have preserved the original end-to-end nature of the Internet, new governance forms such as distributed ledger technologies have started to surface, thanks to technological advances, cost reductions and the possibility to rely on peer-to-peer computing and the power of direct network externalities. Where companies have departed from the original architecture, multi-sided markets have replicated the characteristics of one-to-many communications systems, such as television (e.g. Netflix), and have largely profited from indirect network externalities. The thirst for personal data, coupled with the users' relative lack of awareness of the value of the data they shared and contributed to the working of large-scale algorithms, led these digital intermediaries to prosper by shrinking their size compared to the traditional firm, externalising most functions, reaping advertising benefits and enjoying a largely unregulated space.

Not surprisingly, this first wave of digital transformation created important tensions among regulators, in particular in the European Union. The more digital transformation was permeating traditional markets, the more the differences in the regulatory treatment of incumbent players and digital firms started to tilt the market balance in favour of the latter. The greater the diffusion of data-driven business models, the greater the tensions in terms of data protection, and the loss of control of personal data for end users. The stronger the centripetal forces unleashed by network externalities and platformisation, the greater the polarisation of market power and profits in the hands of a fistful of companies.[19] The more multi-sided platforms conquered the market, the more precarious most workers' conditions became, the more obscure the algorithmic practices behind their selection and reward, and the weaker their access to social dialogue. The greater the imbalance

[19] See T Philippon, *The Great Reversal*, Harvard University Press, 2019.

between firm size and overall profits, the more evident the need for digital taxation based on the place where value is created and revenues are reaped, rather than the place where the digital company is headquartered.

The reaction of the European Union to this first wave of internet transformation was initially very slow, then gradually more assertive and determined. The General Data Protection Regulation, entered into force in May 2018, is the poster child of a generation of reforms that have attempted to restore balance in the digital ecosystem, by establishing principles such as "data minimisation" and "user control over data", which were echoed by legislation in many other legal systems, from Brazil to Japan and California. A regulation on the free flow of non-personal data tried to couple restrictive rules on personal data with expansive rules on non-personal data flows, so far with little impact. Besides antitrust investigations and fine against giants like Google, new regulations expanded the remit of competition rules in areas such as the relationship between platforms and businesses (P2B), echoing national rules on abuse of economic dependence and abuse of superior bargaining power. After interventions on the tax side to counter tax rebates for digital giants such as Apple (in Ireland), work on a web tax has started to take shape, alternating with international efforts in the context of the OECD. And the first attempts to attribute entitlements over data emerged in the field of agriculture, where a code of conduct seeks to empower farmers in reaping value from their data.[20] And the approach to promoting competition in regulated sectors started to move from traditional access obligation related to infrastructure, towards mandatory interoperability obligations, initially imposed on industry incumbents, rather than on tech giants: the case of the Second Payment Services Directive (PSD2) portrays the awakening of the EU institutions to the use of Application Programming Interfaces as a powerful way to impose interoperability obligations, with the (hopefully meaningful) consent of the data subject whose credit data are now moved to third party providers.

Against this background, the Juncker Commission worked also behind the curtains to speed up the reflection on AI rules, on the impact of the digital transformation on labour markets, as well as on the achievement of interoperability between administrations at the EU, national and local level. All these initiatives took the form of expert reflection (through *ad hoc* high-level groups) or voluntary frameworks (as in the case of ISA2); but had the merit to pave the way for an expected acceleration in the coming years, with more binding initiatives. The urgency of a reaction to the evolution of the digital ecosystem was felt more strongly by Member States, leading in some cases the European Commission to adopt initiatives in the attempt to stop the proliferation inconsistent rules at the national level (e.g. for web taxes, as well as for Artificial Intelligence).

Overall, the EU's reaction to the first wave of transformation of the Internet arrived too late, leaving the EU behind other superpowers in terms of preparedness and adaptation to the new paradigms of the digital economy. As acknowledged also by the European Commission, the United States and China have clearly taken the lead on the cloud-dominated, platform-dominated, machine-learning-led digital environment emerged in the past two decades, and only started to concretely react halfway through the Juncker years. The

[20] See A Renda, N Reynolds, M Laurer, G Cohen, *Digitising Agrifood*, CEPS and BCFN joint monograph, 2019.

lack of anticipatory policymaking, for an inevitably cumbersome bloc of 28 states, created a significant lag between the digital transformation and the EU's policy response. That said, once the EU institutions managed to concretely respond, their ability to nest policy proposals into a concrete, solid and comprehensive set of principles led to the emergence of the first real *corpus* of legal rules aimed at creating a more socially and economically sustainable environment for the Internet age. The complete absence of similar rules in most other legal systems made the EU a real pioneer in this policy domain, despite the rather timid approach adopted in several areas. Anu Bradford even sees a magnified "Brussels effect" on global digital policy compared to the many other areas in which the EU already exerts a significant "normative power Europe".[21] This, in turn, encouraged the new European Commission to consider adopting a more assertive approach to digital policy, which culminates in a completely new stance on the Single Market.

1.2. The second transformation wave: the Internet of Things, the rise of Artificial Intelligence and the emergence of distributed architectures

The von der Leyen Commission, already at the end of 2019, took stock of Europe's competition positioning in the digital environment with a degree of despair. Statements on Europe's lag compared to the increasingly battling United States and China proliferated: the world is dominated a fistful of cloud operators, most of which American, none of which European; there are no European companies among the top 20 global tech firms; the data train has left the station, as more than 90% of the data in the Western world are stored in the United States; China is going to dominate 5G, as the US rules the world on platforms and applications; Europe will never manage to match the level of AI investment of the United States and China. However, digital technology never stands still. As policymakers struggle to address the "pacing problem" and respond to the first wave of digital transformation, the evolution of technology is already paving the way for a transformation in the digital environment. And indeed, the next generation if Internet transformation may create new opportunities for Europe to regain its role in the global competition for digital solutions.

In particular, the next few years will mark the blossoming of the Internet of Things (IoT). The physical layer will indeed be enriched by the availability of smart, cyber-physical objects, which can enable decentralised data production, communication and processing, requiring storage and intelligence to be increasingly distributed. The projections of the Internet of Things are breath-taking, with the number of connected objected poised to skyrocket to one trillion by 2035.[22] More specifically, IoT systems are essentially organised around four main (sub-)layers: directly attached to the 'things' are sensors, antennas and actuators, which can take a wide variety of forms; these devices must be connected to a network layer, which allows the aggregation and basic control of data; above these layers (or, as commonly said, above the 'edge') are a first layer of intelligence (Edge IT), which provides analytics functions and pre-processing of data; and the cloud, in which

[21] See Bradford, *op. cit.* And A Renda, Making sense of the "Geopolitical Commission" Insights from the TRIGGER project, CEPS Policy Brief, 2020.

[22] Gros, D. (2019), Global Trends to 2035: Economy and Society, Report for the European Parliament, at http://www.europarl.europa.eu/RegData/etudes/STUD/2018/627126/EPRS_STU(2018)627126_EN.pdf

data are stored, analysed, and processed for ultimate action and decision-making, mostly through Artificial Intelligence.

The IoT revolution will lead to an expansion of the possibility to automate complex processes, but will also require that both data and AI are kept as close as possible to the "things": for example, autonomous vehicles cannot rely on a basic "sensor-to-cloud-and-back" model of thinking, since the fact that data have to travel long distances would generate latency (for every 100 miles, an estimated 0.82 milliseconds). Looking at different network topologies, the immediate alternative to centralised IoT systems would be the implementation of intelligent solutions closer to things, and in particular 'at the edge'. While a fully decentralised system would entail 'embedded AI' in each of the connected objects, and would therefore be too costly using current technologies, most market analysts consider the so-called Edge/Cloud model to be the most interesting paradigm for the most sophisticated IoT use cases in the near future.[23] In an edge/cloud model, local computing, storage, and networking resources are provided close to IoT devices, and the data generated can be stored and pre-processed by the local edge cloud and only a small volume of processed data are eventually sent to central data centres.[24]

As already explained, the conventional cloud models will remain viable for a number of use cases. However, several emerging applications would strongly require an edge/cloud architecture: such a solution can offer important cost savings on top of a more distributed structure.[25] Performing computations at the network edge has several advantages: (i) the volume of data needed to be transferred to a central computing location is reduced because some of it is processed by edge devices; (ii) the physical proximity of edge devices to the data sources makes it possible to achieve lower latency which improves real-time data processing performance; (iii) for the case of data that still must be processed remotely, edge devices can be used to discard personally identifiable information (PII) prior to data transfer, thus enhancing user privacy and security; (iv)

[23] A related term, fog computing, describes an architecture where the 'cloud is extended' to be closer to the IoT end-devices, thereby improving latency and security by performing computations near the network edge. So fog and edge computing are related, the main difference being about where the data is processed: in edge computing, data is processed directly on the devices to which the sensors are attached (or on gateway devices physically very close to the sensors); in fog computing, data is processed further away from the edge, on devices connected using a LAN. See A Renda and M Laurer, *IoT4SDGs. What can the Digital Transformation and IoT achieve for Agenda 2030?*, joint CEPS-Hitachi Report, 2020.

[24] Several attempts have been made at operationalising an edge/cloud model in the past few years. They include projects such as Cloudlet, Nebula, Femtocloud, HomeCloud and Fog Computing. Each of those alternatives has pros and cons, and as occurs for transmission protocols, different solutions may fit different use cases. For example, the implementation of Network Functions Virtualisation and Software-Defined Networking can provide numerous advantages to the dynamic management of edge/cloud systems, especially in the context of 5G deployment.

[25] In 2015, for example, David Floyer studied the data management and processing costs of a remote wind-farm using a cloud-only system versus a combined edge/cloud system. The wind-farm consisted of several data producing sensors and devices such as video surveillance cameras, security sensors, access sensors for all employees, and sensors on wind-turbines. The edge/cloud system turned out to be 36% less expensive and the volume of data required to be transferred was observed to be 96% less, compared to the cloud-only system. D Floyer, "The Vital Role of Edge Computing in the Internet of Things", 2015. Available online at https://wikibon.com/the-vital-role-of-edge-computing-in-the-internet-of-things.

decentralisation can make systems more robust by providing transient services during a network failure or cyberattack; (v) edge computing increases scalability by expanding compute capacity through a combination of edge and IoT devices.

In non-technical terms, it is possible to state that while the AI revolution is the "brain" of the digital ecosystem, and the cloud governs its central nervous system, the IoT will represent the limbs and muscles, and the edge will act as the peripheral nervous system, requiring a degree of automation and fast-thinking already at the local level. This will require a number of important changes in the way the digital economy functions and is organised: small data become more important than big data; data storage occurs mostly at the edge and in devices; and ore distributed architectures are possible, with possible consequences also for competition.

While the edge/cloud architecture will become prominent in the next few years, the B2C world will also see a possible acceleration, in particular through the emergence of more distributed and decentralised architectures, enabling the possibility to store data locally, and in a more privacy-preserving way. The emergence of new paradigms for restoring user control over personal data, from the IHAN project proposed by the Finnish innovation agency SITRA to the approach proposed by the MyData movement and by Tim Berners Lee's Solid project, there is a wealth of ideas for enabling the creation of "data trusts" and other intermediaries, able to help end users easily manage their data by selectively sharing the information they need to share, without losing control of their diffusion in obscure secondary markets.

Most importantly, the new wave of digital transformation promises to achieve very substantial progress in the domain of public services, and more generally in the role of government. Governments that manage to collect good quality data will be able to develop APIs and share them with small and large corporations, researchers and other organisations for the development and provision of value-added services. The new age of "Government as a platform", which saw Estonia as a pioneer with its X-Road ecosystem (now available also in Finland), promises to revolutionise the relationship between public authorities and citizens, and places governments in the driving seat when it comes to securing trust in technology. The upcoming information-rich age will require a strong layer of trusted intermediaries, in charge of verifying the trustworthiness of data flows: suffice it to consider the fast development of "deepfakes", which contribute to an already rich repertoire of disinformation tools by making it almost impossible to distinguish between real and fake audiovisual content.

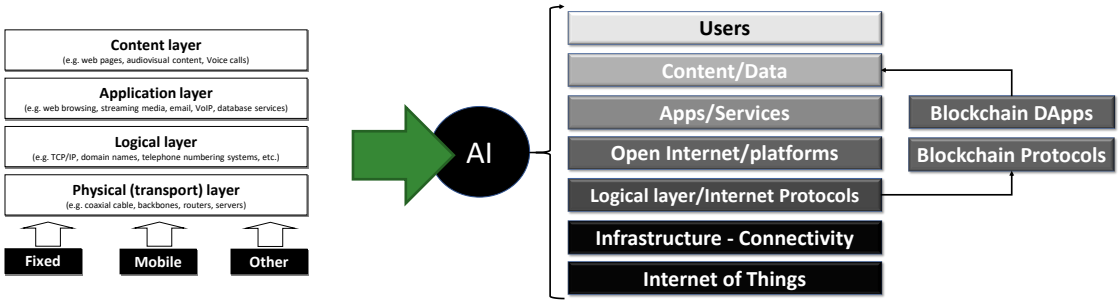
All these developments will determine the final departure of the Internet from its original design, and also away from its current architecture. As occurs in the evolution of complex organisms in biology, here too the Internet will have to accommodate increased complexity due to the co-existence of very different uses, including low-latency industry services enabling control through digital replicas (or "twins"), immersive holographic presence and so-called "multi-sense media", alongside with more traditional data flows. Inevitably, the giant technology companies of today may have an advantage in conquering also those spaces,

which explains to a large extent why they continue investing huge sums in R&D. At the same time, the competitive space is open to new players, and even more to investment by private and public institutions that, from the "real economy", seek the achievement of a more balanced and sustainable internet architecture. This is where the European Union may have an advantage over other superpowers, and even vis à vis the current tech giants.

1.3. Wrapping up: an evolving ecosystem

The past few years have been characterized by the rise of a new wave of technological developments, which promise to revolutionize the digital economy, bringing it towards and era dominated by dramatically superior computing power and connectivity speeds; a skyrocketing number of cyber-physical objects connected to the Internet (the so-called Internet of Things, or IoT, powered by nano-technology and by 5G wireless broadband connectivity); and the pervasive spread of artificial intelligence into almost all aspects of personal and professional life. This new stack will be composed of powerful hardware, including faster processors (mostly a combination of CPUs, GPUs and TPUs); distributed computing capacity through edge (or fog) computing; new, distributed and decentralized platforms such as blockchain, able to keep audit trails of transactions and other asset-backed values; and a pervasive presence of AI-enabled solutions, mostly in the form of data-hungry techniques such as smart analytics, deep learning and reinforcement learning.[26] Focusing on all layers of this emerging stack is extremely important when it comes to scaling up these technologies to the benefit of society: merely focusing on one element, such as AI or blockchain, would not harness the full potential of this emerging world.

Figure 1. The old v. new digital technology stack



Source: Author's elaboration

Figure 1 above portrays the evolution of the technology stack. The Internet of Things (IoT) layer generates an unprecedented amount of data, requiring sensor technology, nano-tech, enhanced connectivity through 5G or satellite, and devices like drones or robots, able to generate live data remotely[27]. Regardless of the way

[26] See A Renda, *Artificial Intelligence: Ethics, Governance and Policy Challenges*. CEPS Monograph, 2019.

[27] Data can be stored in various ways, including through remotely accessible, cloud-enabled solutions; through distributed databases; or through distributed ledger technologies such as blockchain. Some of these technologies are

in which data are generated, stored and exchanges, the use of AI will be ubiquitous in most supply chains. At the top of the supply chain, end users very often constitute the "weakest" link, which require the provision of adequate skills in using digital technologies (Renda 2019).

Although no real estimate of the combined impact of these technologies on the future economy exists, several studies have already been published on the economic impact of AI, as well as on the impact of IoT in specific sectors. For example, recent reports by Accenture/Frontier Economics, McKinsey and PWC conclude that AI will be a game changer for total factor productivity and growth, by gradually rising as a third pillar of production, together with labour and capital. PWC concluded that by 2030, global GDP will be 14% higher due to AI development and diffusion;[28] the Accenture study finds that growth rates will be doubled by 2035 thanks to AI.[29] The latter study also shows an industry-by-industry breakdown, which includes agriculture, forestry and fisheries: this sector is expected to more than double its growth rate by 2030, from 1.3% to 3.4% on a yearly basis thanks to AI. Distributed ledger technologies are expected to complement these developments by solving several market failures along supply chains, as well as empowering end users in their consumption choices; some commentators go beyond these expectations and foresee a revolutionary impact of blockchain in many sectors, but this chiefly depends on whether more decentralised architectures will prove scalable over time.

2. Towards Single Market 2.0: a vision for the future of EU digital policy

The reaction of the European Union to the rise of the digital economy was initially very slow, then gradually more assertive and determined. The General Data Protection Regulation, entered into force in May 2018, is the poster child of a generation of reforms that have attempted to restore balance in the digital ecosystem, by establishing principles such as "data minimisation" and "user control over data", which were echoed by legislation in many other legal systems, from Brazil to Japan and California. A regulation on the free flow of non-personal data tried to couple restrictive rules on personal data with expansive rules on non-personal data flows, so far with little impact. Besides antitrust investigations and fine against giants like Google, new regulations expanded the remit of competition rules in areas such as the relationship between platforms and businesses (P2B), echoing national rules on abuse of economic dependence and abuse of superior bargaining power. After interventions on the tax side to counter tax rebates for digital giants such as Apple (in Ireland, later overturned by the Court of Justice), work on a web tax has started to take shape, alternating with

key enablers of value chain integrity, monitoring and trust, since they produce "audit trails" that enhance the verifiability of transactions and contractual performance across the value chain.

[28] PWC (2017), "Sizing the Prize. What's the real value of AI for your business and how can you capitalise?", PWC Analysis (https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf).

[29] Purdy, M. and P. Dougherty (2017), "Why Artificial Intelligence is the Future of Growth", Accenture/Frontier Economics Report (https://www.accenture.com/t20170927T080049Z__w__/usen/_acnmedia/PDF-33/Accenture-Why-AI-is-the-Future-of-Growth.PDFla=en).

international efforts in the context of the OECD. And the first attempts to attribute entitlements over data emerged in the field of agriculture, where a code of conduct seeks to empower farmers in reaping value from their data.[30] And the approach to promoting competition in regulated sectors started to move from traditional access obligation related to infrastructure, towards mandatory interoperability obligations, initially imposed on industry incumbents, rather than on tech giants: the case of the Second Payment Services Directive (PSD2) portrays the awakening of the EU institutions to the use of Application Programming Interfaces as a powerful way to impose interoperability obligations, with the (hopefully meaningful) consent of the data subject whose credit data are now moved to third party providers.

Against this background, the Juncker Commission worked also behind the curtains to speed up the reflection on AI rules, on the impact of the digital transformation on labour markets, as well as on the achievement of interoperability between administrations at the EU, national and local level. All these initiatives took the form of expert reflection (through *ad hoc* high-level groups) or voluntary frameworks (as in the case of ISA2); but had the merit to pave the way for an expected acceleration in the coming years, with more binding initiatives. The urgency of a reaction to the evolution of the digital ecosystem was felt more strongly by Member States, leading in some cases the European Commission to adopt initiatives in the attempt to stop the proliferation of inconsistent rules at the national level (e.g. for web taxes, as well as for Artificial Intelligence).

Overall, the EU's reaction to the first wave of transformation of the Internet arrived too late, leaving the EU behind other superpowers in terms of preparedness and adaptation to the new paradigms of the digital economy. As acknowledged also by the European Commission, the United States and China have clearly taken the lead on the cloud-dominated, platform-dominated, machine-learning-led digital environment emerged in the past two decades, and only started to concretely react halfway through the Juncker years. The lack of anticipatory policymaking, for an inevitably cumbersome bloc of 28 states, created a significant lag between the digital transformation and the EU's policy response. That said, once the EU institutions managed to concretely respond, their ability to nest policy proposals into a concrete, solid and comprehensive set of principles led to the emergence of the first real *corpus* of legal rules aimed at creating a more socially and economically sustainable environment for the Internet age. The complete absence of similar rules in most other legal systems made the EU a real pioneer in this policy domain, despite the rather timid approach adopted in several areas. Anu Bradford even sees a magnified "Brussels effect" on global digital policy compared to the many other areas in which the EU already exerts a significant "normative power Europe".[31] This, in turn, encouraged the new European Commission to consider adopting a more assertive approach to digital policy, which culminates in a completely new stance on the Single Market.

[30] See A Renda, N Reynolds, M Laurer, G Cohen, *Digitising Agrifood*, CEPS and BCFN joint monograph, 2019.

[31] See Bradford, *op. cit.* And A Renda, Making sense of the "Geopolitical Commission" Insights from the TRIGGER project, CEPS Policy Brief, 2020.

The von der Leyen Commission, already at the end of 2019, took stock of Europe's competition positioning in the digital environment with a degree of despair. Statements on Europe's lag compared to the increasingly battling United States and China proliferated: the world is dominated a fistful of cloud operators, most of which American, none of which European; there are no European companies among the top 20 global tech firms; the data train has left the station, as more than 90% of the data in the Western world are stored in the United States; China is going to dominate 5G, as the US rules the world on platforms and applications; Europe will never manage to match the level of AI investment of the United States and China. However, digital technology never stands still. As policymakers struggle to address the "pacing problem" and respond to the first wave of digital transformation, the evolution of technology is already paving the way for a transformation in the digital environment. And indeed, the next generation if Internet transformation may create new opportunities for Europe to regain its role in the global competition for digital solutions.

In particular, the next few years will mark the blossoming of the Internet of Things (IoT). The physical layer will indeed be enriched by the availability of smart, cyber-physical objects, which can enable decentralised data production, communication and processing, requiring storage and intelligence to be increasingly distributed. The projections of the Internet of Things are breath-taking, with the number of connected objected poised to skyrocket to one trillion by 2035.[32] More specifically, IoT systems are essentially organised around four main (sub-)layers: directly attached to the 'things' are sensors, antennas and actuators, which can take a wide variety of forms; these devices must be connected to a network layer, which allows the aggregation and basic control of data; above these layers (or, as commonly said, above the 'edge') are a first layer of intelligence (Edge IT), which provides analytics functions and pre-processing of data; and the cloud, in which data are stored, analysed, and processed for ultimate action and decision-making, mostly through Artificial Intelligence.

The IoT revolution will lead to an expansion of the possibility to automate complex processes, but will also require that both data and AI are kept as close as possible to the "things": for example, autonomous vehicles cannot rely on a basic "sensor-to-cloud-and-back" model of thinking, since the fact that data have to travel long distances would generate latency (for every 100 miles, an estimated 0.82 milliseconds). Looking at different network topologies, the immediate alternative to centralised IoT systems would be the implementation of intelligent solutions closer to things, and in particular 'at the edge'. While a fully decentralised system would entail 'embedded AI' in each of the connected objects, and would therefore be too costly using current technologies, most market analysts consider the so-called Edge/Cloud model to be the most interesting paradigm for the most sophisticated IoT use cases in the near future.[33] In an edge/cloud

[32] Gros, D. (2019), Global Trends to 2035: Economy and Society, Report for the European Parliament, at http://www.europarl.europa.eu/RegData/etudes/STUD/2018/627126/EPRS_STU(2018)627126_EN.pdf

[33] A related term, fog computing, describes an architecture where the 'cloud is extended' to be closer to the IoT end-devices, thereby improving latency and security by performing computations near the network edge. So fog and edge computing are related, the main difference being about where the data is processed: in edge computing, data is processed directly on the devices to which the sensors are attached (or on gateway devices physically very close to the sensors); in fog computing, data is processed further away from the edge, on devices connected using a LAN. See A Renda and M Laurer, *IoT4SDGs. What can the Digital Transformation and IoT achieve for Agenda 2030?*, joint CEPS-Hitachi Report, 2020.

model, local computing, storage, and networking resources are provided close to IoT devices, and the data generated can be stored and pre-processed by the local edge cloud and only a small volume of processed data are eventually sent to central data centres.[34]

As already explained, the conventional cloud models will remain viable for a number of use cases. However, several emerging applications would strongly require an edge/cloud architecture: such a solution can offer important cost savings on top of a more distributed structure.[35] Performing computations at the network edge has several advantages: (i) the volume of data needed to be transferred to a central computing location is reduced because some of it is processed by edge devices; (ii) the physical proximity of edge devices to the data sources makes it possible to achieve lower latency which improves real-time data processing performance; (iii) for the case of data that still must be processed remotely, edge devices can be used to discard personally identifiable information (PII) prior to data transfer, thus enhancing user privacy and security; (iv) decentralisation can make systems more robust by providing transient services during a network failure or cyberattack; (v) edge computing increases scalability by expanding compute capacity through a combination of edge and IoT devices.

In non-technical terms, it is possible to state that while the AI revolution is the "brain" of the digital ecosystem, and the cloud governs its central nervous system, the IoT will represent the limbs and muscles, and the edge will act as the peripheral nervous system, requiring a degree of automation and fast-thinking already at the local level. This will require a number of important changes in the way the digital economy functions and is organised: small data become more important than big data; data storage occurs mostly at the edge and in devices; and more distributed architectures are possible, with possible consequences also for competition.

While the edge/cloud architecture will become prominent in the next few years, the B2C world will also see a possible acceleration, in particular through the emergence of more distributed and decentralised architectures, enabling the possibility to store data locally, and in a more privacy-preserving way. The emergence of new paradigms for restoring user control over personal data, from the IHAN project proposed by the Finnish innovation agency SITRA to the approach proposed by the MyData movement and by Tim Berners Lee's Solid project, there is a wealth of ideas for enabling the creation of "data trusts" and other

[34] Several attempts have been made at operationalising an edge/cloud model in the past few years. They include projects such as Cloudlet, Nebula, Femtocloud, HomeCloud and Fog Computing. Each of those alternatives has pros and cons, and as occurs for transmission protocols, different solutions may fit different use cases. For example, the implementation of Network Functions Virtualisation and Software-Defined Networking can provide numerous advantages to the dynamic management of edge/cloud systems, especially in the context of 5G deployment.

[35] In 2015, for example, David Floyer studied the data management and processing costs of a remote wind-farm using a cloud-only system versus a combined edge/cloud system. The wind-farm consisted of several data producing sensors and devices such as video surveillance cameras, security sensors, access sensors for all employees, and sensors on wind-turbines. The edge/cloud system turned out to be 36% less expensive and the volume of data required to be transferred was observed to be 96% less, compared to the cloud-only system. D Floyer, "The Vital Role of Edge Computing in the Internet of Things", 2015. Available online at https://wikibon.com/the-vital-role-of-edge-computing-in-the-internet-of-things.

intermediaries, able to help end users easily manage their data by selectively sharing the information they need to share, without losing control of their diffusion in obscure secondary markets.

Most importantly, the new wave of digital transformation promises to achieve very substantial progress in the domain of public services, and more generally in the role of government. Governments that manage to collect good quality data will be able to develop APIs and share them with small and large corporations, researchers and other organisations for the development and provision of value-added services. The new age of "Government as a platform", which saw Estonia as a pioneer with its X-Road ecosystem (now available also in Finland), promises to revolutionise the relationship between public authorities and citizens, and places governments in the driving seat when it comes to securing trust in technology. The upcoming information-rich age will require a strong layer of trusted intermediaries, in charge of verifying the trustworthiness of data flows: suffice it to consider the fast development of "deepfakes", which contribute to an already rich repertoire of disinformation tools by making it almost impossible to distinguish between real and fake audiovisual content.

All these developments will determine the final departure of the Internet from its original design, and also away from its current architecture. As occurs in the evolution of complex organisms in biology, here too the Internet will have to accommodate increased complexity due to the co-existence of very different uses, including low-latency industry services enabling control through digital replicas (or "twins"), immersive holographic presence and so-called "multi-sense media", alongside with more traditional data flows. Inevitably, the giant technology companies of today may have an advantage in conquering also those spaces, which explains to a large extent why they continue investing huge sums in R&D. At the same time, the competitive space is open to new players, and even more to investment by private and public institutions that, from the "real economy", seek the achievement of a more balanced and sustainable internet architecture. This is where the European Union may have an advantage over other superpowers, and even vis à vis the current tech giants.

The emerging new technology stack will be composed of powerful hardware, including faster processors (mostly a combination of CPUs, GPUs and TPUs); distributed computing capacity through edge (or fog) computing; new, distributed and decentralized platforms such as blockchain, able to keep audit trails of transactions and other asset-backed values; and a pervasive presence of AI-enabled solutions, mostly in the form of data-hungry techniques such as smart analytics, deep learning and reinforcement learning.[36] Focusing on all layers of this emerging stack is extremely important when it comes to scaling up these technologies to the benefit of society: merely focusing on one element, such as AI or blockchain, would not harness the full potential of this emerging world.

The Internet of Things (IoT) layer generates an unprecedented amount of data, requiring sensor technology, nano-tech, enhanced connectivity through 5G or satellite, and devices like drones or robots, able to generate

[36] See A Renda, *Artificial Intelligence: Ethics, Governance and Policy Challenges*. CEPS Monograph, 2019.

live data remotely[37]. Regardless of the way in which data are generated, stored and exchanges, the use of AI will be ubiquitous in most supply chains. At the top of the supply chain, end users very often constitute the "weakest" link, which require the provision of adequate skills in using digital technologies (Renda 2019).

Although no real estimate of the combined impact of these technologies on the future economy exists, several studies have already been published on the economic impact of AI, as well as on the impact of IoT in specific sectors. For example, recent reports by Accenture/Frontier Economics, McKinsey and PWC conclude that AI will be a game changer for total factor productivity and growth, by gradually rising as a third pillar of production, together with labour and capital. PWC concluded that by 2030, global GDP will be 14% higher due to AI development and diffusion;[38] the Accenture study finds that growth rates will be doubled by 2035 thanks to AI.[39] The latter study also shows an industry-by-industry breakdown, which includes agriculture, forestry and fisheries: this sector is expected to more than double its growth rate by 2030, from 1.3% to 3.4% on a yearly basis thanks to AI. Distributed ledger technologies are expected to complement these developments by solving several market failures along supply chains, as well as empowering end users in their consumption choices; some commentators go beyond these expectations and foresee a revolutionary impact of blockchain in many sectors, but this chiefly depends on whether more decentralised architectures will prove scalable over time.

In this context, the EU is faced with the herculean task of shifting gear towards a more assertive and enlightened policy for the Digital Single Market, in a way that preserves its values and at the same time boosts its competitiveness and sustainability over the coming years. This will require a thorough redefinition of the strategy for the Single Market, to preserve at once its role of "workhorse" of European integration, as well as driver of EU international actorness and competitiveness. The European Commission has acknowledged in many occasions that there can be no "geopolitical Commission" without a strong Single Market at home: even strategies aimed at orienting digital technology towards human rights and sustainability require a significant market positioning to be credible in internal fora.

As already mentioned, the "new" European Commission made a strong commitment to the digital transition, positioning the digital environment as a critical infrastructure, and postulating the need for digital sovereignty and the twin transition (green and digital) as cornerstones of its new geopolitical mission. The adoption of a comprehensive, ambitious data strategy and the White Paper on Artificial intelligence paved the way for new policy developments that aim, for the first time, at anticipating future market developments by achieving a

[37] Data can be stored in various ways, including through remotely accessible, cloud-enabled solutions; through distributed databases; or through distributed ledger technologies such as blockchain. Some of these technologies are key enablers of value chain integrity, monitoring and trust, since they produce "audit trails" that enhance the verifiability of transactions and contractual performance across the value chain.

[38] PWC (2017), "Sizing the Prize. What's the real value of AI for your business and how can you capitalise?", PWC Analysis (https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf).

[39] Purdy, M. and P. Dougherty (2017), "Why Artificial Intelligence is the Future of Growth", Accenture/Frontier Economics Report (https://www.accenture.com/t20170927T080049Z__w__/usen/_acnmedia/PDF-33/Accenture-Why-AI-is-the-Future-of-Growth.PDFla=en).

first-mover advantage in the forthcoming second wave of digital transformation. As clearly stated by Commissioner Thierry Breton, the European Commission expects that the next years will mark a transition towards more distributed, localised data storage, at the edge and in devices as opposed to the cloud. While cloud operators will remain important, they will be part of a more complex architecture, as we described in Section I.2. This represents at once a challenge and an opportunity: on the one hand, it is clear that Europe has missed the first train (the B2C wave), and this may deprive it of the resources, the skills and the industrial base needed to jump into the second; on the other hand, the B2B sector is not (yet) dominated by the large tech giants, and requires the orchestration of resources from legacy industrial sectors, such as manufacturing, automotive, pharma, energy, in which European corporations are often market leaders. Similarly, the importance of data flows in (and for) government require action to avoid that public institutions end up relying on non-EU players for cloud and software solutions: digital sovereignty thus calls for new initiatives aimed at creating a full European technology stack. As explained by the European Commission, this assertive approach can and should be coupled with concrete commitments to use digital technology "for good", in particular in support of the Green transition: this requires, for example, that data centres become carbon neutral by 2030, and that the IT equipment used in Europe aligns with the requirements of the circular economy.[40]

The COVID-19 pandemic created a double challenge to the original commitments of the von der Leyen Commission. On the one hand, the need for concrete actions to strengthen Europe's digital economy has become even stronger, as most economic and social activities move online: an investment in the IoT and the Edge IT layers appears urgent to say the least, in the attempt to transform suffering economic sectors, facing an unprecedented nosedive in production and turnover. On the other hand, the upcoming depression may lead those sectors in dire straits, and thereby in the impossibility to embark in such an ambitious transformation. Despite the crisis situation, at the time of writing EU institutions have confirmed their intention to proceed as planned on the twin transition: the Council conclusions of 26 March 2020 urged the Commission to "get back to a normal functioning of our societies and economies and to sustainable growth, integrating inter alia the green transition and the digital transformation, and drawing all lessons from the crisis."[41]

The Commission's response on the twin transition placed the Single Market at the forefront, advocating the acceleration towards a "more circular, climate neutral and modernised economy". Current emphasis is however being placed on incremental measures such as reinforcing digital skills and making new tools and resources available to SMEs, on the reduction of red tape, the strengthening of enforcement in the traditional Single market. Only time will tell whether Breton's original ides of a more forward-looking approach to the Digital Single Market will survive the COVID-19 crisis. In order for Europe to realise its ambition to preserve

---

[40] See the European Commission's Communication, Shaping Europe's Digital Future, 19 February 2020, at https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf.

[41] See Joint Statement of the Members of the European Council, 26 March 2020, at https://www.consilium.europa.eu/media/43076/26-vc-euco-statement-en.pdf.

and further nurture its actorness and competitiveness at the global level, it is important that the Commission realises that the "data train" has not left the station, and that Europe has a unique window of opportunity to rely on the new digital transition to boost its weight in global economy. This requires a number of initiatives, aimed at rebalancing (or restoring) competition in B2C digital markets; create and promote efficient data spaces in the B2B domain; pave the way for a distributed and reliable single market for services; enable a network of interoperable administrations and leverage eIdentity as a means to empower citizens and consumers; and lead the world on the responsible development and use of digital technologies.

Below, I briefly elaborate on each of those pillars.

2.1.1. Rebalancing competition and value allocation in the B2C domain: from competition policy to the federated cloud infrastructure

It has become relatively uncontroversial that the "first wave" of digital transformation has created positions of excessive power, transforming a fistful of digital players in gatekeepers of the Internet, and leading to an excessive concentration of value generated by the digital economy.[42] There are many ways in which the EU institutions can try to rebalance this situation.

First, the Commission is likely to reform its competition rules to acknowledge the existence of specific situations in which digital players, regardless of market definition, occupy a position that grants them "intermediary" power, mostly fuelled by network effects and data availability. This move, which would echo the recent debate on the German draft Digitalisation Bill, might lead to considering specific remedies, such as the imposition of mandatory interoperability for specific datasets, to enable competitors to deploy similar services. This is likely at least for specific datasets which can be considered to be essential to develop services of general interest, and would be a re-proposition of the essential facilities doctrine, which dates back more than two decades in EU competition law, to cases like *Magill*, *IMS Health*, and *Microsoft*.[43]

Second, in the B2C domain, EU institutions could decide to go beyond data access and interoperability obligations, and adopt policies aimed at returning control of their data to end users, or even treat data 'as labour' whenever possible, as advocated recently by the Report of the High Level Expert Group on the Impact

[42] See M Mazzucato, *The Value of Everything. Making and Taking in the Global Economy*, Penguin Books, 2018.

[43] See A Renda, "Competition-regulation Interface in Telecommunications. What's left of the Essential Facilities Doctrine", *Telecommunications Policy*, Vol. 34, Issues 1-2, February-March 2010, at 23-35. Based on this approach, whenever a dominant market player holds an asset of information that is essential for competitors to viably compete in the relevant market, and refusal to provide access to this information is likely to either lead to the exit, or even prevent the growth of, 'as efficient' or even 'not yet as efficient' competitors, then competition law may provide for compulsory access remedies. Much in the same vein, the German government is now imposing compulsory access obligations to tech giants for specific datasets. In a recent paper for the European Commission's DG COMP, Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer echo this view by observing that "the ability to use data to develop new, innovative services and products is a competitive parameter whose relevance will continue to increase"; and clarified that "in a number of settings, data access will not be indispensable to compete, and public authorities should then refrain from intervention. In other settings, however, duties to ensure data access – and possibly "data interoperability" – may have to be imposed". The paper correctly points out that a "broader diffusion of data is not always desirable, either from a social welfare or from a competition perspective" due to privacy concerns; and that in addition to data interoperability, in some cases full protocol interoperability may be needed for competitors to be able to compete on an equal footing.

of the Digital Transformation on EU Labour Markets.[44] This would lead to forms of remuneration from digital platforms to end users, which may take various forms, including the provision of free services, or most likely a web tax, which seems even more likely in the aftermath of the COVID-19 pandemic.[45] This approach, however, would not lead to the creation of more competition in the market, or possibly even the entry of European players in the B2C segment.

Another area that will prove important to rebalance the bargaining position of market players and users in the ecosystem is the effective implementation of recent EU rules on the unfair distribution of the contractual surplus among parties in the commercial relation. So-called "platform-to-business" (P2B) practices have been subject to specific regulation in the European Union, where a specific observatory on online platforms has been created in order to monitor the application of the regulation. The EU P2B regulation introduces a ban on certain unfair practices (e.g. no more sudden, unexplained account suspensions, plain and intelligible terms and advance notice for changes, greater transparency and mandatory disclosure for a range of business practices) and new dispute resolution possibilities.[46] P2B rules echo similar legislation that many countries have enacted in the domains of abuse of economic dependency, abuse of superior bargaining power, contract law, or unfair competition. In Germany, the draft Digitalisation Bill echoes existing provisions on "relative market power" vis-á-vis smaller enterprises, by removing any reference to the business size and adding that relative market power shall also be assumed for "undertakings acting as intermediaries on multi-sided markets insofar as undertakings are dependent on their intermediary services with regard to access to supply and sales markets in such a way that sufficient and reasonable alternatives do not exist" (Sec. 20 para. 1 GWB-Draft).[47]

Apart from reforming existing rules, the Commission will also act to restore digital sovereignty in the ecosystem, in particular by seeking the creation of a federated cloud infrastructure, operating under rules and protocols that embed strict data protection and governance requirements. This will most likely take inspiration from the GAIA-X project, initiated by France and Germany and already including more than 120 partners. GAIA-X can be seen as the quintessential pan-European approach to the future of the Single Market: rather than representing a single player competing with the US tech giants, GAIA-X is a federated data infrastructure, open to small and large companies, which attempts at once to level the playing field, and to embed in the cloud specifications the compatibility with key European provisions on security, data protection,

---

[44] See the Final report of the High-Level Expert Group on the Impact of the Digital Transformation on EU Labour Markets, April 2019, at https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-impact-digital-transformation-eu-labour-markets..

[45] In that case, the tax would be based on the consideration that the digital platforms derive (some would say, extract) value from the end users, who provide data in exchange for being part of the platform: the main theoretical argument in favour of such a form of redistribution is the 'collective action problem' faced by end users, who are structurally unable to place a price on the data they provide, while these data, once aggregated, become extremely valuable to the platform. This form of positive externality could be seen as the market failure that a web tax, or any other form of redistribution, would seek to remedy

[46] In Australia, similar concerns were expressed during the ACCC Digital Platforms Inquiry. Among those practice, some may also lead the digital platform to favour its own products, or anyway "preferred" customers on the business side, possibly through algorithmic ranking and product placement choices.

[47] Relative market power is to be assumed if undertakings depend on access to data to enter a market; in addition, hampering rivals' attainment of positive network effects can constitute an abuse if this is capable of triggering the tipping of a market: this includes case in which a platform adopts measures measures to disable data portability or interoperability along with exclusivity clauses or tying practices, to the extent that such measures create a "serious risk of a considerable restriction of competition on the merits."

openness and transparency, interoperability and trust. In particular, interoperability is sought at three different infrastructure levels: network, data and service, in a way that resembles the approach to interoperability adopted by the European Commission to enhance exchanges between EU and national administrations (see below).

While still in its infancy, the GAIA-X project represents a gateway towards a next generation approach to technology-enabled policymaking at the EU level. It is, in particular, a clear response to the emerging edge-cloud infrastructure (as acknowledged in the GAIA-X White Paper);[48] and a sign of the increased awareness, in the European Commission, of the revolutionary potential of the second wave of digital transformation: centralized governance does not mean market concentration, especially if a common environment for cloud services is coupled with clear data interoperability and portability rules. In this respect, the emphasis on common standards and a thicker (three-level) interoperability framework embeds the key features of the Single Market 2.0 approach, in continuity with a long-standing approach of the European Commission.

2.1.2. Securing the B2B domain: the end of open data

Based on our description of the EU strategy above, it is inevitable that the strongest effort of the new Commission will be concentrated in the B2B domain, where the emergence of the IoT and the edge/cloud infrastructure powered by 5G and other forms of connectivity call for a new approach to industrial policy. This seems to lead to a combination of data strategy and industrial policy, both adopted by the von der Leyen Commission under the auspices of Commissioner Breton in the first 100 days of the Commission's mandate.

The data strategy announces the objective to create a single European data space and couple it with measures aimed at ensuring that by 2030, the EU's share of the data economy corresponds to its economic weight ("not by *fiat* but by choice", the Commission adds). The idea of creating a "genuine single market for data" leads to an upgrade of the "free flow of non-personal data" approach that emerged during the Juncker Commission. Even if the Commission is very cautious not to venture into too assertive statements, it emerges clearly that in the B2B domain, the age of "open data", free-flowing information as a means to the promotion of innovation is definitely over. The need to avoid capture of industrial data by large tech giants, and imbalances in the distribution of revenues along the value chain, leads the Commission to propose the creation of a two-layer architecture, with an overarching single European data space and a number of domain- or mission-specific data spaces. The stated reasons for this move are the fragmentation between national data policies, and the persistence of significant constraints to all types of data flows; the existence of imbalances of market power; problems of data quality and interoperability; lack of adequate provisions for data governance; and a collection of other problems on both the supply and the demand side of data, including security aspects, regulatory certainty, and skills.

[48] See Project GAIA-X. A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem. Available at https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.pdf?__blob=publicationFile&v=4.

The result is the proposed creation of a series of large pools of data in specific domains, combined with the technical tools and infrastructures necessary to use and exchange data, as well as appropriate governance mechanisms. These pools (renamed "data spaces") require the adoption of a horizontal framework complemented by sectoral legislation for data access and use, and mechanisms for ensuring interoperability, and must be developed in full compliance with data protection rules and according to the highest available cyber-security standards. Such framework will be adopted by the end of 2020, and will need to be complemented by policies that stimulate the use of data and demand for services enriched with data.[49] Apart from the governance aspects of data space management, which are still unknown, it is clear that data spaces are a key component of the Commission's new vision for data-driven industrial policy, and aim at realising at once a rebalancing effect (keep entitlements over data in the hands of industrial players) and a repatriation effect (ensure that data are stored and managed according to European rules, and preferably in the territory of the EU).

The data spaces proposed by the Commission in its data strategy, as already mentioned, are in some cases cross-sectoral, in others more sector-specific. Among the cross-sectoral ones are a "Green Deal data space", which is expected to mobilise public and private data to help achieve Europe's environmental goals, even by creating a digital twin of the Earth; a Common European skills data space, aimed at reducing skills mismatches in the labour market; and European data spaces for the public administration, aimed at strengthening data exchanges, promoting transparency and accountability, fighting corruption, and enabling GovTech solutions. More sectoral solutions are devoted to manufacturing, mobility, health, finance, energy and agriculture.

The data spaces approach must be analysed in conjunction with the Industrial Strategy communications, adopted by the Commission in March 2020.[50] The strategy, though mostly focused on the real economy and on related topics such as innovation and entrepreneurship as well as industry alliances and the "analogue" Single Market, places strong emphasis on the concept of industrial ecosystems, which are not clearly defined in the Communication. One of the most crucial aspects of the new ecosystems approach is whether they will be defined as coinciding with industry sectors (e.g. aviation), or in a mission-oriented way (e.g. mobility). Data spaces have been defined according to the latter approach, but the COVID-19 crisis may call for a more sector-specific approach to industry support and aid. The new approach to the Single Market 2.0 would preferably preserve the mission-oriented approach, as well as its vocation towards sustainable development in a technology-neutral way.

[49] See the Commission's Work Programme 2020 at https://ec.europa.eu/info/publications/2020-commission-work-programme-key-documents_en.

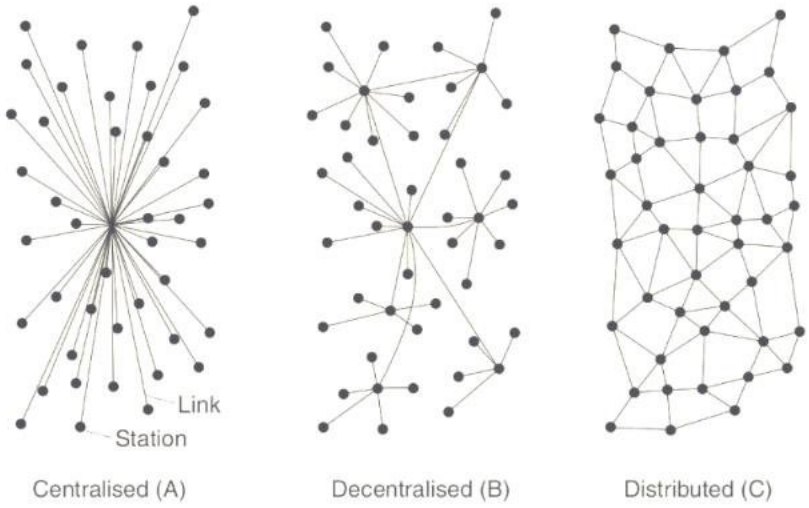
[50] See Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, "A New Industrial Strategy for Europe", COM(2020)102 final, 10 March 2020.

2.1.3. A distributed single market for services

Above the infrastructure and data governance layers, the Single Market 2.0 will enable different forms of governance, from centralised to more distributed and decentralised. One interesting characteristic of the digital economy, in this respect, is that the traditional barriers to entry in the form of economies of scale are less likely to materialise, especially in the service economy. The servitisation of the economy describe in Section I above makes it possible for very small businesses to use powerful IT equipment, rent drones and even tractors or other costly machinery "as a service". The rise of 3D printing decentralises the production and assembling of products, drastically reducing costs. For example, in agriculture communities of farmers can then access modern technology at a fraction of the cost, and only for the time needed.[51] However, as already recalled these barriers to entry are being replaced by less tangible ones, notably represented by data access and management, as well as related skills.

The new technological frontier, coupled with interoperability rules, will make further servitization possible, alongside with the adoption of more distributed governance structures, thereby enabling greater market competition. Industrial economics will fundamentally change, unveiling the possibility to address issues in a centralised, distributed or decentralised way, as depicted in figure 2 below. In some cases, a centralised architecture (for example, exclusively cloud-based) may emerge, thereby triggering network externalities and winner-take-all competition; in other situations, a decentralised structure may lead to edge/cloud architectures and federated structures organised along a limited number of "supernodes"; and finally, with technological development even fully distributed structures, with service provision among peers, become increasingly possible.

Figure 2 – Centralised, decentralised and distributed computing



[51] See Renda *et al.*, *Digitising Agrifood*, op. cit.

Source: Truong et al. (2016)[52]

In more concrete terms, this may mean that in some markets, a large number of small corporations may end up competing for services, by using data made available through widespread interoperability requirements. This comes very close to the IHAN model proposed by SITRA, which *de facto* re-proposes the PSD2 "open API" approach at a wider scale, commoditising data availability (hopefully, implementing privacy-preserving arrangements) and laying the foundations for a more competitive, pluralistic Single Market for services. Maximising data availability will also mean liberating all possible sources of data flow, including the use of public sector information by business (G2B); sharing and use of privately-held data by other companies (B2B); the use of privately-held data by government authorities when appropriate and desirable (B2G); and data-sharing between public authorities (G2G). In this respect, all other pillars of the proposed new framework for the Single Market 2.0 are essential to feed the new services market. For example, public administrations (as defined in more detail below) could enable innovation by acting as platforms and offering open APIs to citizens and businesses, thereby significantly lowering the data barrier to entry. Widespread, privacy-compatible data availability throughout the Union can also contribute to the environment by enabling more localised solutions. In a nutshell, the Single Market 2.0 would be more integrated (through data flows), competitive (through data interoperability), decentralised (through lower data barriers to entry) and environmentally sustainable (through lower transport costs, as well as carbon-neutral data centres).

Such a vision requires, inevitably, the support of modernised legal rules. In particular, the scope of most product liability regimes does not include intangible goods, implying that cases of inadequate services, careless advice, erroneous diagnostics and flawed information are as such not covered. A comparable situation exists in the field of product safety regulation, which so far has not been accompanied by a regulatory framework in the field of safety of services. In all these fields, the EU *acquis* appears far from complete, and will require more attention in the years to come. The upcoming Digital Service Act should fill this gap by clarifying the conditions for the liability of online service providers and intermediaries. The needed update of the Product Liability Directive will most certainly entail a revision of key definitions such as "product" and "producer", as well as rules on certain practices adopted by service providers vis à vis end users, such as price personalisation through automated decision-making and profiling. In other words, the body of rules that supports the new vision of the Single Market should be able to generate sufficient trust among end users, as will be explained in more detail in Section II.5 below.

2.1.4. Digital government and e-identity

Data availability and user-centric innovation in the future Single Market 2.0 would greatly benefit from a proactive role of government in the generation, collection, protection and provision of data. This can occur through *ad hoc* data trusts, or simply by public administrations acting as orchestrators of the data economy.

[52] N Truong, U Jayasinghe, T-W Um and M Gyu, "A Survey on Trust Computation in the Internet of Things", *The Journal of Korean Institute of Communications and Information Sciences* (J-KICS) 33, 10-27, 2016.

The European Commission has gone a long way in creating the preconditions for the interoperability between administrations in Europe, in particular through its ISA2 programme, which led to the development of re-usable building blocks, available to national and local governments on a purely voluntary basis. However, that framework has led to a very low uptake, and would need to be converted into a much more concerted action for the development of digital government and "government as a platform" approaches in Europe: this includes measures included in the semester, in the InvestEU and Digital Europe programmes, and dedicated support through the newly created DG REFORM. The swift transition towards digital government solutions is even more urgent since the Ministerial Declaration on e-Government in Tallinn on 6 October 2017, in which the Ministers in charge of e-Government policy from 32 countries of the European Union (EU) and the European Free Trade Area (EFTA) unanimously committed to the vision laid out in the EU e-Government Action Plan 2016-2020 and in the new European Interoperability Framework that public administrations and public institutions in the EU should be open, efficient and inclusive, providing borderless, interoperable, personalised, user-friendly, end-to-end digital public services to all citizens and businesses – at all levels of public administration[53]. This includes, i.a., the development of more efficient and user-centric digital services; a call on the EU institutions to develop more interoperable, efficient, open and transparent administrative procedures to best serve their citizens and interoperate with all levels of government[54]. The ISA2 programme will leave, as important legacy, a layered approach aimed at building the foundations of the Single Market 2.0 by ensuring a high level of legal, organisational, semantic and technical interoperability between administrations.

EU institutions should take the timeline of the Tallinn declaration seriously: they have agreed at the end of 2017 to achieve six targets within five years: digital by default and inclusiveness; application of the "once only principle"; secure trusted electronic identification and trust services for electronic transactions in the internal market; enable the possibility for people and business to access personal data held by the public administrations; integrate instruments and a call to public authorities to oblige cross-border interoperable solution compatibles with European frameworks and standards; and improve the digital leadership skills and the IT education in every level of the public administrations.[55]

Among these commitments, as particularly important for the development of the whole Single European data space will be the area of digital verification, encompassing both digital identify (eID) and electronic trust services (eTS), altogether subsumed under an EU framework for authentication in digital transactions (eIDAS). eIDAS sets the standards and criteria for simple electronic signature, advanced electronic signature, qualified electronic signature, qualified certificates and online trust services. Furthermore, it rules electronic transactions and their management. Among other benefits, it fully recognizes digital means of verification that are considered to be equivalent to physical presence. In doing so, it lays the foundations for the creation

[53] https://ec.europa.eu/digital-single-market/en/news/ministerial-declaration-egovernment-tallinn-declaration

[54] Id.

[55] https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/news/tallinn-egov-declaration

of the Single European Data space. The system could in the future be updated to include other means of verification (e.g. fingerprint scan) and create a new system for certification of digital ID in the Single Market 2.0. It should also be complemented by trustless (or better, trust-enhancing) mechanism for time-stamping, origin-stamping and other transaction authentication methods offered by Distributed Ledger Technologies (including fully privacy-preserving ways such as zero knowledge proofs).

2.1.5. Leading the world on digital technology "for good"

As already remarked in the previous section, a key pillar of the emerging Single Market 2.0 will necessarily have to be the trustworthiness of its infrastructure, protocols, rules, and services. In this respect, the EU has the responsibility and the opportunity to lead the world in the development of a trusted digital environment and has already started to do so in the domain of Artificial Intelligence. In the AI field, the European Commission (backed by an *ad hoc* High-Level Expert Group (AI HLEG), advocated the transition towards "Trustworthy Artificial Intelligence", defined as AI that meets three cumulative requirements: legal compliance, ethical alignment, and socio-technical robustness. The AI HLEG identified four key principles (defined as ethical "imperatives") for Trustworthy AI: the respect for human autonomy, the prevention of harm, fairness and explicability[56]. These principles were further broken down into seven requirements, which were then operationalized into an Assessment List on Trustworthy AI (ALTAI). This strategy arrived at a turning point with the White Paper adopted on February 19, 2020 (together with the new EU strategy for data), in which the von der Leyen Commission announces the adoption of a flexible, agile regulatory framework limited to 'high-risk' applications, in sectors such as healthcare, transport, police and the judiciary; and focusing on provisions related to data quality and traceability, transparency and human oversight. A legislative initiative on AI is now expected by the end of 2020, as outlined in the Work Programme of the European Commission, which envisages a follow-up to the White Paper, including on safety, liability, fundamental rights and data.

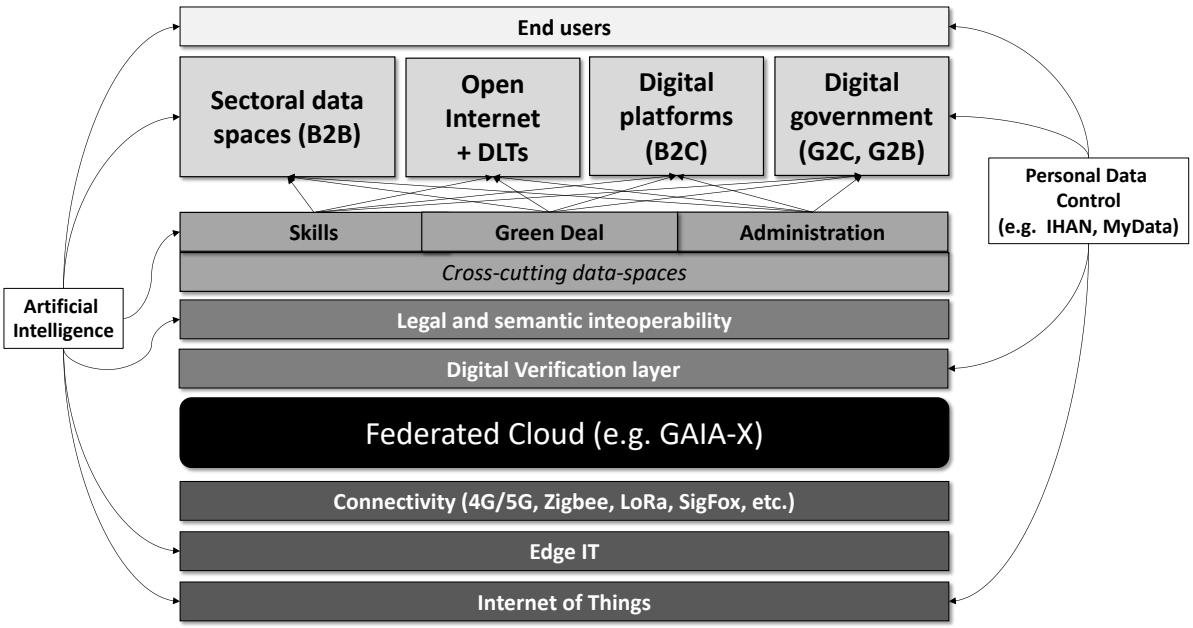
The EU agenda on AI inspired many other countries and international organisations, including the OECD principles on AI, the G20 human-centred AI Principles, as well as the "AI for good" within the International Telecommunications Union. This revived the EU's actorness in the digital technology space, where it is now a recognized standard-setter, and perhaps the only superpower able to credible orchestrate a dialogue on responsible uses of digital technologies (starting with AI). In order to sustain high standards in this domain, as already recalled, the EU will need to rely on a vibrant Single Market, to be leveraged through extra-territorial rules to avoid that EU products are outcompeted by non-European, less sustainable standards.

[56] Importantly, contrary to what typically occurs in similar documents, the list did not include an imperative to "do good", or the so-called "beneficence" principle, which had been included in earlier drafts of the Guidelines See A Jobin, M Ienca, E Vayena, The global landscape of AI ethics guidelines. Nature Machine Intelligence (ISSN 2522-5839). September 2, 2019.

2.1.6. Towards a new architecture for the Single Market 2.0: a sketched architecture of the evolving layered ecosystem

The five pillars of the Single Market 2.0 illustrated in Section II are certainly a non-exhaustive account of the possible future of Europe's "crown jewel". Compared to the architecture of the Internet shown in Figure 1 above, the new Single Market would look more articulate, but not necessarily more complex from an end user perspective. As shown in figure 3, the Single Market 2.0 would have an extensive infrastructure layer, composed of connected things, the edge IT layer, various connectivity protocols (including 5G and many others) and the federated cloud infrastructure. Above that layer, the traditional logical layer would be flanked by a legal, identity/trust and semantic interoperability layer, which will then support the emerging cross-cutting and sector-specific data spaces. These will cover most of the Single Market 2.0 from a B2B perspective, whereas the B2C will be more similar to the current Internet ecosystem. An important role could be played by G2C and G2B services with public administration becoming real catalysts of social innovation.[57]

Figure 3 – A sketched architecture of Single Market 2.0



Source: Renda (2020)

This, inevitably, is only a sketch of the main components of the future Single Market 2.0, which will certainly be even more complex. The role of technologies such as blockchain and other DLTs in enabling transactions and fostering the so-called token economy is one of many aspects that will emerge over the next few years, and which are difficult to fully anticipate at the time of writing. The digital environment, as I have tried to explain throughout these pages, is an ever-changing multi-layered ecosystem, which becomes thicker as time

[57] See also AI HLEG, Policy and Investment Recommendations, June 2019.

goes by, and where the technological evolution defines the frontier of what is possible in a constantly evolving way.

More specifically, in the coming months EU institutions will have to define an effective, new regulatory governance for digital technologies, as key for the realisation of "Single Market 2.0". The main ingredients of this emerging recipe are listed below.

- **Trust: towards a new regulatory governance model.** The EU has made significant progress in the definition of a common framework for regulating digital technologies, even if most of the initiatives appear still sparse and partly inconsistent. The most advanced and comprehensive framework, in this respect, is the one designed by the High-Level Expert Group on AI, which by defining "trustworthy artificial intelligence" ended up laying the foundations of a more general definition of (and approach to) trustworthy digital technology. Such definition encompasses three key dimensions: legal compliance, ethical alignment, and socio-technical robustness, which possibly apply to all digital technologies, beyond AI. Realising this framework also for other digital technologies, including data spaces and the federated cloud, would greatly enhance EU's credibility and cohesion by premating the whole *acquis* of an additional layer of policy coherence.
- **An optimal balance between innovation and precaution, through flexible and adaptive regulatory schemes.** The emerging regulatory framework on AI was presented as "risk-based", i.e. developers and deployers of AI are held accountable for gauging the risks that they could generate for society, and adopt corresponding and proportionate mitigating measures. Requiring this enhanced level of attention recalls the formula of Judge Learned Hand, according to which negligence (and this liability) is assessed based on the relation between investment in precaution and the product of the probability and magnitude of harm resulting from an accident. However, the AI HLEG also clarified that whenever the potential risks of developing or deploying a given AI application or system are difficult or impossible to predict, and are possibly catastrophic, then the precautionary principle should apply.[58] The constant oscillation between a precautionary approach and a more innovation-friendly, less cautious regulatory approach has been the subject of a constant debate over the past years, with some commentators arguing that Europe's strong regulatory frameworks stifle innovation, and others that praise the ability of regulation to give direction to innovation (Ashford and Renda 2016). In reality, the most advanced literature in this domain has shown a much more nuanced reality than a systematic greater precaution in EU regulation when compared to US one (Wiener et al. 2011; IRGC 2019). In addition, Europe's already-recalled peculiar balance between ex ante regulation and ex post enforcement (in particular through litigation) inevitably calls for greater ex ante scrutiny of products and services that reach the market, an aspect that is often neglected by academics and policymakers when comparing the two systems. An emerging opportunity for the EU would be the promotion of a more agile, flexible and adaptive policy approach, which does not compromise on the level of precaution considered to be optimal for the specific technology at hand. This can be achieved by a combination of actions, which include the strengthening of EU's ability to experiment with policy and technology solutions, i.a. through so-called "sandboxes" (if properly designed); the creation of agile governance mechanisms, such as a public-private board in charge of defining and

[58] Ethics Guidelies for Trustworthy AI.

updating requirements for trustworthy digital technology, including data quality and ethics standards; and the introduction of so-called "GovTech" or "RegTech" solutions, which embed legal rules "as code" in common technical specifications to be applied throughout the territory of the Union (see below).

- **Foresight: keep megatrends and technological developments in sight.** Breton's anticipation of the shift from a cloud-dominated to an edge-dominated environment, especially for what concerns data storage, is an almost unprecedented attempt of the EU to anticipate future developments and engage in so-called anticipatory policymaking (Nesta 2017). For the EU to strengthen its role of global standard-setter in the digital domain, this approach should be strengthened and made more systematic. This is indeed in the plans of the von der Leyen Commission, especially as the better regulation agenda and foresight are being merged under the responsibility of vice President Sefcovic. The EU could then follow the example of other countries, such as Singapore with its Centre for Strategic Futures, and Canada with its Policy Horizon initiative, in the attempt to strengthen its ability to identify risks and anticipate future trends. After the COVID-19 pandemic, this activity is also being approached from the perspective of increasing Europe's resilience, i.e. the ability of the European society and economy to absorb unforeseen shocks. The EU post-COVID-19 plan is oriented towards this dual perspective of resilience and recovery, under the assumption that public policies should "protect, prepare and transform" society and the economy towards enhanced sustainability and prosperity. In this latter respect, foresight-based policymaking is also an important precondition for matching public policy decisions with expected outcomes, such as the achievement of the Sustainable Development Goals. Understanding long-term scenarios (on which, see also Section 3.3 below) also means developing a greater awareness of the risks and opportunities that will present themselves on the way to achieving the ultimate vision for Europe in 2030 and beyond.
- **Openness, but not at all costs.** While openness has been a poster child of the first three decades of information technology policy at the European level (well represented by Commissioner's Moedas "Open Science, open innovation, open to the world" slogan), the von der Leyen Commission has quickly realised that the natural appeal of the concept is not reflected in the desirability of its practical implementation. Open standards, in an economy dominated by large tech giants, can crystallise the uneven value distribution observed in the platformisation of the Internet. By strengthening network effects in parts of the ecosystem that complement digital platforms, open standards can strengthen the market power of the largest players: this peculiarity of an otherwise commendable approach towards openness is visible also in the ultimate impact of theoretically sacrosanct policy initiatives such as net neutrality rules. Future EU policy should thus pursue openness, but not at all costs: rather, open data flows will be gradually replaced by a system of managed, shared data within data spaces, and entitlements over data will be placed in the hands of real economy players, especially in the industrial context, to avoid the gradual capture of key industrial data and know-how by large technology firms. To use a metaphor, a data lake is certainly not an open sea. And data spaces should not primarily be construed to maximise the transfer of data from industry players to over-the-top intermediaries.
- **Beyond legal rules: standardisation and "embedded" regulatory governance.** As discussed in this section, one of the key challenges for the future of EU policy is the need to gradually abandon traditional forms of regulation, and translate EU principles and laws into standards

> and ultimately software code, i.e. technical software specifications to be applied as a precondition for operating in the European market. On the one hand, standards are crucial to make sure new technologies such as AI and DLTs / blockchain develop in a way that is compatible with the values of liberal democracies: respect for human rights, privacy, accountability, and transparency. Standards should be proactively developed in Europe to enable auditing of applications of blockchain/DLTs and AI, as is happening in the context of conformity assessment, possibly leading to forms of certification and auditing. This is also happening in GAIA-X, which gathers network and interconnection providers, cloud solution providers, high-performance computing as well as sector-specific clouds and edge systems around common minimum technical requirements and services, nested *i.a.* in the principles of Security by Design and Privacy by Design.[59] A similar "compliance by design" approach, which echoes Lessig's "perfect technology of justice" and places it at the service of EU's technological sovereignty, will most likely be adopted also in the design of the cross-cutting and sectoral data spaces, as well as in future specifications for smart government. The ISA2 programme developed by the European Commission within the European Interoperability Framework is indeed the foundry in which the notion of conceptual reference building blocks with embedded compliance by design was originally forged.[60]

Time will tell whether the EU institutions will realise this ambitious plan, which would project the EU into a more sustainable future; and whether technological sovereignty will be approached by the EU as a way to strengthen its own resilience, or also as a bargaining chip in a revived setting of international collaboration, especially with transatlantic partners. Developing common regulatory approaches with partners such as the US, Canada, and the UK ensures that liberal democratic values are embedded in technologies being developed in all of these countries and that the open, transparent, and accountable approach forms a real counterweight to the closed, intrusive, government-controlled approach to technological development favoured by some authoritarian countries.

---

[59] The technical implementation of these services will indeed focus on areas such as the implementation of secure federated identity and trust mechanisms; sovereign data services which ensure the identity of source and receiver of data and which ensure the access and usage rights towards the data; easy access to the available providers, nodes and services, with the provision of data through federated catalogues; the integration of existing standards to ensure interoperability and portability across infrastructure, applications and data; the establishment of a compliance framework and Certification and Accreditation services; and the contribution of a modular compilation of open source software and standards to support providers in delivering a secure, federated and interoperable infrastructure. See https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html.

[60] https://ec.europa.eu/isa2/actions/towards-european-interoperability-architecture_en.

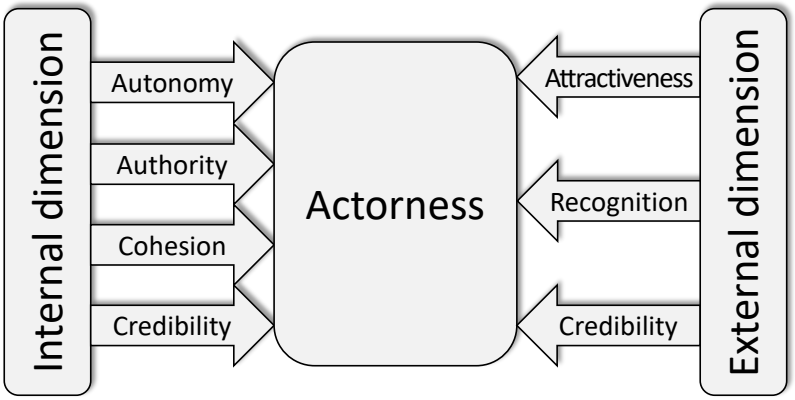
3. Europe in the digital economy: enhancing EU actorness and effectiveness in the face of possible future scenarios

The direction and scope of EU digital policy will also significantly affect Europe's ability to preserve and consolidate its reputation of global standard-setter, which according to some commentators applies also in the digital sphere (Bradford 2019; Kalff and Renda 2019). Today, Europe seems to face new opportunities in this domain, also due to the decline of the United States as the leading country in the promotion of competitive markets (Philippon 2019), as well as with the erosion of American "soft power", mostly as a result of the Trump administration's lack of enthusiasm for international cooperation (Nye Jr. 2019). The US retreat from multilateralism, with fading support for organisations such as the WTO and the IMF, is leaving an important trace on the ability of the world' first economy to lead by example and export its values to the rest of the world. As a matter of fact, the European Union today stands as the only global superpower that has the potential to credibly lead the world on key global issues such as sustainable development, global warming and the responsible use of digital technologies.

Against this background, the notion of "power", as well as other concepts such as "agency", "influence" and "legitimacy" have been used to analyse the EU's capability to act independently. The TRIGGER project, following a consolidated stream of literature, decided to focus on the least normative of these concepts, i.e. "actorness" as a necessary (but not sufficient) precondition for "effectiveness" in global governance. Actorness has been defined in various ways depending on the author and the policy domain.[61] TRIGGER therefore adopts a comprehensive definition of actorness (see figure 4), which is made dependent on a variety of internal and external factors.

Figure 4 – The TRIGGER conceptual model of actorness

[61] The explanatory variables of actorness have revolved around various theoretical concepts and notions, with frequent overlaps and overall, a certain confusion. Already in 1977, Sjöstedt introduced the concept of actorness as the "capacity to behave actively and deliberately in relation to other actors in the international system": notably, this concept does not immediately entail the ability to influence others, or to impose one's own agenda. Other authors, such as Hill (1993, 1998), Bretherton and Vogler (2005) and Jupille and Caporaso (1999), point at a number of determinants of actorness, such as internal cohesion, coherence (as coordination between EU policies), consistency between internal and external policies, capacity in terms of policy levers and resources, opportunities and presence in the international system, autonomy (including authority) and external recognition. Other authors (i.a. Kratochvil et al. 2011) highlight the internal and external factors that determine EU's actorness. And more recently, Klose (2018) defines actorness in terms of role-playing, i.e. as "an entity's capacity to re-imagine and realize roles for its 'self' in (specific contexts of) international affairs".



Source: Elaboration based on Jacob et al. (2019)

The TRIGGER definition captures the major dimensions highlighted in the literature, avoiding the difficult and controversial conceptualisation of the actor's power.[62] The definition also contemplates possible overlaps and interdependencies between the various internal and external determinants. For example, authority and autonomy may often be correlated, since the existence of specific EU competences in the Treaty typically triggers the allocation of funding in the EU budget; autonomy, at least for the part that refers to the capability to act, may be related also with cohesion; and cohesion may in turn be a determinant of credibility and trust. Similarly, for external factors, attractiveness is unlikely in the absence of recognition. At the same time, there are possible interlinkages between internal and external factors: opportunity may be weakened by the lack of capability to act, or the lack of autonomy. As a result, the proposed formula for actorness should not be taken as a sum of internal and external factors, but rather as a conceptual framework, which can help track the evolution of various determinants of actorness over time and, if consistently applied, lead to a meaningful comparison of actorness across policy areas.

[62] The notion of actorness per se was coined to reflect the specific condition of the European Union, which escapes the mechanistic application of concepts such as sovereignty, legitimacy, or power. Almost three decades ago, John Ruggie (1993) referred to the EU as a "collectivity acting as a singularity", as well as a "multiperspectival" and "quasi-formed" polity. Since them many other authors have offered explanations and definitions, ranging from the EU as a new kind of state, as a non-state political system, as a new type of international organisation or as a traditional type of international organisation (Leruth and Lord 2017). The degree of complexity increases in other contributions: for example, Sergio Fabbrini (2015) sees in the EU the co-existence of different systems, including an economic Union, an intergovernmental Union, a parliamentary Union and a monetary Union, following either a Community method, or a Union method.

The conceptual framework illustrated in this section can and should also be interpreted in a dynamic and relative way. As a matter of fact, actorness can change over time and is essentially a relational concept, in the sense that an actor does not exist in isolation, and actorness is never an absolute metric, but is rather dependent on the evolution of other players' actorness in the specific governance space. Likewise, actorness appears to be tightly linked to a two-dimensional set of variables: on the one hand, the expectations raised on the possibility frontier of EU action; on the other hand, the capacity and behaviour that the EU deploys in the policy space. As a result, as the expectations on the EU keep expanding, past strategies may not be considered sufficient, or adequate anymore, and the EU is called to adapt its conduct to the new reality, or new perceptions, of its potential as a global actor.

Against this background, and also based on the analysis in three key domains of digital policy carried out by TRIGGER researchers, it is possible to perform a first assessment of EU's actorness and effectiveness in the digital domain.

3.1. EU Actorness in the digital economy: a preliminary analysis

The EU appears to have a significant degree of actorness in the digital economy, with important margins for improvement. Below, I explore the main findings of the TRIGGER papers on digital technology, and add some considerations related to the overall thrust and direction of EU policy in this domain.

3.1.1. Internal dimensions

3.1.1.1 Authority

Authority is defined as the EU's legal competences in a specific area, as laid out in the treaties or in issue-specific agreements. The TRIGGER papers found a number of positive elements that contribute to a high degree of authority, thanks also to the fact that Member States have gradually conferred more competences to the EU level over time. Straightforward examples are: the transition from a Directive to a Regulation in the field of privacy and data protection, which further harmonises the EU approach to an important policy domain, in which the EU is credited with the definition of global standard-setter; and the upcoming introduction of a pan-European data spaces and a regulation on AI, which promise to further harmonise EU law in emerging, strategic areas.[63]

On the positive side, the EU's strong competences on data protection contribute to greater actorness also in other domains, such as those aspects of AI/ML and those areas of OSS and open standards governance that are covered by the GDPR. In addition, the introduction and forthcoming revision of a Coordinated Plan on AI, joint with an effort in streamlining conformity assessment and impose specific regulatory requirements on high-risk AI applications, is likely to strengthen EU's authority in this domain in the years to come. In the domain of distributed ledger technologies, authority is more difficult to appraise, but there are encouraging

[63] The EU's new data strategy (European Commission 2020) and the upcoming legislative initiative on the governance of data spaces move away from informal coordination between the Commission and the member states by bringing more competences to the EU level (see, e.g., Prinsley et al. 2020).

signs of a gradual conferral, if not of powers, at least of the right of initiative from the national level to the EU level. For example, in finance Member States seem to have taken the stand of waiting to see what the European Union does first before regulating on a national level, underscoring EU's authority in the governance of blockchain and distributed ledger technologies. And in the field of e-identity and authentication, the European Commission has taken important steps in its attempt to achieve interoperability between administrations and common standards across Europe (e.g. EIDAS), which is perceived as being extremely complementary to the development of blockchain solutions, particularly on self-sovereign identity.

On the negative side, EU competences are limited in a number of key policy domains. For example, the treaties do not contain an explicit competence relating to OSS or open standards.[64] This is also reflected in a low level of authority on public procurement, an area that accounts for close to 20% of the EU GDP; and could otherwise be leveraged as a market-creating opportunity. This means that the EU cannot direct national governments to purchase Trustworthy AI solutions, adopt distributed ledger technologies, purchase open source software or technologies that implement open standards: however, Collins and Florin (2020) argue that the EU could claim authority to act in this area based on one specific treaty provision, namely the functioning of the single market.

More generally, the vision of a Single Market 2.0 is one in which the EU has greater authority in the digital domain. Such greater authority is achieved largely by shifting to the EU level the responsibility for launching digital solutions and governance frameworks that pursue, sometimes as an ancillary objective, the goal of streamlining and harmonising rules and standards across the EU27. Greater authority is thus achieved by the EU both as a traditional regulator (e.g. in AI) and as a legitimate "orchestrator" of cloud federations and data spaces.

3.1.1.2 Autonomy

Autonomy, in TRIGGER's definition, has little connection to the ideas of "strategic autonomy" or "technological sovereignty" that are constantly evoked as pillars of the new "geopolitical" Commission. Rather, it refers to the EU's capacity (including its resources) to set its own priorities and act independently of the member states. In this domain, the TRIGGER papers highlighted the relatively low capacity of EU institutions to leverage resources that are comparable to the levels of investment observed in China, or the United States. In particular in the domain of AI, the EU has included most of the funding in the forthcoming "Digital Europe" programme, which will be able to rely on no more than 6.7 billion Euros for the 2021-2027 financial framework. At the same time, the Commission outlined its ambition to reach 20 billion Euros of investment in AI per year, but this figure contains possible commitments of the Member States and the private sector, as part of the so-called Coordinated Plan on AI. While these commitment may seem insufficient for the EU to keep the pace of other large countries (the prospective investment goals equal

[64] The European standardization organizations provide another arena for informally promoting OSS. For example, ETSI (2019) signed a memorandum of understanding with the Linux Foundation last year, and the European Commission published a joint report with the Open Forum Europe (2017) recently, in order to make sure that OSS developers implement standards and that SDOs adopt OSS development methodologies.

roughly the yearly R&D spending at Amazon only), it is also true that many of the other budget lines available in the EU budget, from space to Horizon Europe, may bring additional resources to invest in AI. One notable example is the announced European Alliance for Industrial Platforms and Cloud co-funded by Member States and supported by EU institutions with an investment of approximately 2 billion Euros and will launch *i.a.*, an Important Project of Common European Interest (IPCEI) for a European edge/cloud platform.[65]

For what concerns other technology areas, Mattila (2020) finds it unlikely that blockchain technology and DLTs would be exhaustively directly legislated on by the European Union: EU actorness thus "somewhat hinges on the national supervisory entities in the matter": the only exception is potentially found in areas such as e-identity, authentication and verification of transactions, as well as in the data space for public administrations, where in the future funding could be made available to pursue market integration initiatives. According to an IDC published in 2019, the EU was expected to spend $674 million on blockchain in 2019; whereas the U.S. had an expected spend of $1.1 billion, and China of $319 million in the same year. In the domain of open source and open standards, the limited ability of EU institutions to leverage public procurement as a demand-side innovation policy can limit the EU's autonomy.

All in all, it seems reasonable to conclude that the level of autonomy in the domain of digital technologies is limited, mostly due to insufficiently ambitious spending plans. At the same time, the human resources available to the Commission are significant, with 840 staff members in DG CONNECT, as well as dedicated personnel in DG GROW, DG JUST, DG HOME, DG RTD and in the Joint Research Centre.[66] These human resources are however increasingly dealing only with policy issues, with the exception of a number of remaining funding channels (e.g. the Next Generation Internet).

3.1.1.3 Cohesion

Cohesion, in the TRIGGER model, refers to the level of consistency between EU and member state institutions, but also between different EU institutions and in general within the EU *acquis*. While cohesion seems to be relatively low in the case of blockchain and Distributed ledger Technologies, in particular due to the different levels of awareness and support for these technologies observed in the Member States and even in EU institutions, for other digital technologies there seems to be a clear tendency towards a consistent approach.

In the domain of open standards and OSS, there appears to be broad alignment on the value of increasing governments' use of OSS and open standards. However, Büthe and von Ingersleben-Seip (2020) observe that despite their overall commitment, EU institutions admitted informally to be still captive to Microsoft software; at the same time, the European Interoperability Framework has remained largely a voluntary scheme until now, and the Commission also gradually moved away from requiring that any IP contained in open standards be licensed for free. In line with the general deviation from open data and open standards, towards

[65] See Breton, 23 June 2020.

[66] https://ec.europa.eu/info/sites/info/files/european-commission-hr_key_figures_2020_en.pdf

more "managed" standards and data governance, the future data space for public administration may contain a number of provisions on the compulsory licensing and sharing of IP, as well as on the use of common, interoperable (but not necessarily open) standards.

In the domain of AI, cohesion was very low until recently, in 2018, when the Coordinated Plan on AI was launched by the European Commission. Likewise, the forthcoming adoption of a regulatory framework for AI is likely to strengthen cohesion within the EU, contributing positively to EU actorness. At the same time, the implementation and enforcement phases of the policy cycle feature a significant heterogeneity amongst the EU27, including in more consolidated fields such as the GDPR (as demonstrated by the recent review by the European Commission); and in key domains such as liability for emerging technologies. There, besides EU legislation on product safety and liability, which appears harmonized and broadly suited to address most of the concerns raised by AI and IoT products (but still in need of an update), the real problem is the fragmentation of national rules on civil liability. National non-harmonised regimes, as observed by the Commission, feature fault-based liability rules, according to which victims of damage need to prove the fault of the liable person, the damage and causality between the fault and the damage in order to establish a successful liability claim; and in some cases strict liability regimes (more correctly, relative strict liability, i.e. a strict liability regime that contemplates cases of exemption, with a reversal of the burden of proof) where the national legislator has attributed liability for a risk to a specific person, without the need for a victim to prove fault/defect or causality between fault/defect and the damage.[67]

Looking more broadly at the EU *acquis* in the domain of digital technologies, a number of areas feature a degree of inconsistency and fragmentation in the Member States. These include i.a. spectrum policy, broadband penetration, cybersecurity governance, and many more.

[67] For example, in the case of road traffic accidents some systems rely on fault-based liability in general (Malta for example) or in limited circumstances, such as in the case of a collision (Poland for example); or for certain types of damage (Spain); and some systems make the application of the traffic liability regime conditional on the involvement of a driver (Italy); some systems exclude passengers from protection under strict traffic liability, either in general (Greece or the Netherlands for example keeper is excluded from compensation) or only in specific circumstances (i.a. Poland or Austria). In the case of smart home devices, similar considerations apply. Some countries (such as Spain or Greece) can use their special regimes of liability for flawed services, based on a presumed fault on the service provider's part. Other legal systems operate solely or mainly on the basis of their general provisions on fault liability (general clauses) or relatively open tort law concepts (tort of negligence, breach of statutory duty). Some legal systems (Germany, Austria, or Greece, and to some extent Denmark, for example) extend contractual liability under certain conditions, allowing a third party to invoke a contract they were not a party to themselves. This applies to situations where the contract is deemed to establish duties to also protect such third parties, allowing the latter to sue for compensation in cases of breach. Protected third party must be foreseeably close to the contracting partner, though, confronted in a similar way with the danger stemming from non-performance (such as family members or guests). Any kind of contractual liability is, however, usually subject to contractual (and sometimes also statutory) limitations. Similarly, complex situations may result in cases where damage was caused by autonomous healthcare applications. Such damage would usually be subject to fault-based liability, either in contract or in tort. Further complexities arise from the interplay between these regimes and social insurance and/or healthcare systems.

All in all, it is reasonable to conclude that the level of cohesion in the EU digital policy is on the rise, but is still showing important potential for improvement. The Von der Leyen Commission seems determined to achieve progress, but only time will tell whether this will ultimately and effectively occur.

3.1.2. External dimensions

3.1.2.1 Recognition

In the TRIGGER conceptual framework, recognition refers to international perceptions of the EU in a given governance domain. Thus, recognition of a particular actor is high when the actor in question is viewed as an influential actor or an important negotiating partner in a particular domain. Overall, recognition appears to be relatively high for the EU, seen as a global standard-setter in the digital domain. There are many potential reasons for this exposure, beyond the mere observation of a rather significant legislative activity.

First, while the United States (and to some extent also China and South Korea) have adopted a rather light regulatory framework, the European Union has gradually reacted to the initial "hands-off" approach vis à vis the digital economy, at times for reasons of necessity (e.g. in the regulatory framework for e-communication), and in other occasions responding to a genuine need to restate its values in an environment dominated by private governance (i.e. the GDPR). More generally, the EU often needs to regulate on specific issues to avoid that fragmented national initiatives hamper the Single Market (e.g. as in the case of AI, or digital taxation); and as a compromise between different legal systems and traditions. The latter feature of EU law make it already quite palatable for non-EU countries, which may found easier to adapt EU law to their context compared to US or Chinese solutions. Moreover, many developed and developing countries around the world share with the EU the legal tradition (both common and civil law), often as part of a colonial past. Finally, EU legislation is also often more structured and systematic than US legislation, also given that the US often rely on lighter ex ante regulation and a more substantial apparatus for ex post litigation compared to European countries, and this in turn makes their policy frameworks more difficult to replicate elsewhere compared to EU ones.

In the three specific domains analysed by TRIGGER, recognition was moderate or high. In particular, EU policies served as a global example on open standards during the 2000s, but then the momentum for EU standard-setting in this domain seems to have slowed down: as noted by Büthe and von Ingersleben-Seip (2020), "the European Union's open source activism seems to have died down somewhat over the last few years", as confirmed by the fact that the Commission's open source strategy has not been updated since 2017. Moreover, EU's activism in the domain of intellectual property for global standards, however justified, has reportedly weakened the recognition of the EU in the domain of open source and open standards governance. On the side of AI, despite a rather fragmented governance landscape, the external recognition of the work of the European Commission and the High Level Expert Group on AI has been significant, and the emerging regulatory framework for AI is seen as a possible global standard in particular, the ethics guidelines on Trustworthy AI produced by the HLEG have been the basis for the OECD principles, and later the G20

principles on AI and the newly launched Global Partnership on Artificial Intelligence. However, this extraordinary recognition from a regulatory perspective must be gauged against the clear leadership of US and China on the use of AI to drive innovation and growth.

Lastly, the EU seems to enjoy strong recognition also in the domain of blockchain and DLTs, even if the international governance landscape for these technologies is still rather under-developed. One way in which the EU is seeking to increase its role in this space is by acting as promoter and orchestrator of INATBA, the international association of trusted blockchain applications launched in April 2019, which already included fron the start 106 organisations representing the full DLT ecosystem. INATBA was launched and is hosted at the European Commission headquarters, and is strongly supported also by the World Bank, the OECD, the UN World Food Program, UNFCCC, UNICEF, the European Investment Bank, the European Bank for Reconstruction and Development. The initiative for INATBA came from several participants in the EU Blockchain Industry Round Table, a European Commission hosted group, which has been working to identify the right conditions for blockchain technologies to flourish.

In summary, the recognition of the EU's role and influence in digital technology policy is significant but undermine by the rather weak investment prospects compared to other countries. All in all, the EU seems on its way to increasing its recognition by further strengthening its commitment to principles-based and outcome-based policy in areas where the EU will be a real pioneer, such as the regulation of high-risk AI applications.

3.1.2.2 Attractiveness

Attractiveness is determined primarily by the extent to which external actors perceive it as advantageous to cooperate with the EU in a given policy area. It is, as a result, a heavily volatile dimension, which may depend on factors that are completely independent of the strategies and policy initiatives undertaken by the EU. For example, 2020 say a sudden rise in the US interest in reviving the transatlantic dialogue on digital policies, which testifies of a growing consideration of the EU as an attractive partner and a necessary ally. This, besides the EU's acknowledged progress in this field, seems to be motivated mostly by growing concerns in the US about the rise of China as a global superpower in this field. In related fields, such as data protection and governance, the negotiations on the adequacy of the data protection regimes of important third countries such as Japan and India show the level of attractiveness of the EU as a partner, in particular due to the sheer size and wealth of Europe's single market, and the strong texture and quality of its legislative framework. GDPR is gradually been "copied" in other parts of the world, from Japan to California and Brazil. Europe's competition cases and rather rigid regulatory frameworks on the digital economy have led important industry leaders to visit Brussels to discuss issues related to regulation. At the same time, Europe's relatively low innovation and investment in this domain undermines its potential attractiveness in the face of global partners.

More specifically, among the areas analysed in the TRIGGER project, the attractiveness of the EU in the domain of open standards and open source software is quite high, also since the EU is viewed as an "important and influential cooperation partner in standard-development processes", and because the EU holds many key secretariat positions in international standard development organizations. Countries are attracted to the EU to co-develop technologies that become certified standards and are therefore adopted by a wide variety of market participants; and also due to Europe's extensive technical knowledge and vast experience in developing standards. Here again, EU's attractiveness depends on a continued commitment to (and success in) the development of global standards in key emerging technolgoies such as AI, 5G and the Internet of Things.

In this latter respect, Collins and Florin (2020) find that the EU does not rank highly for attractiveness in AI, since the "leadership of the US and China on innovation and growth gives them higher levels of attractiveness in terms of potential material gain". They find a similarly low attractiveness also in the EU's data strategy, even if initiatives such as GAIA-X could be a strong future driver of attractiveness.

In the areas of blockchain and DLTs, Mattila (2020) observes that "the vast range of different initiatives in which the European Union has engaged in can be considered to increase the actorness of the European Union in this regard", via a greater attractiveness over time. This is also due Europe's success in fostering innovation ecosystems around blockchain and DLTs: future actions, especially in the financial sector and in the data space on public administration, may make Europe "the" place to develop blockchain solutions in the future.

3.1.2.3 Opportunity/necessity to act

Opportunity and necessity to act represent another external dimension of actorness, and perhaps the most time- and context-dependent one. In the digital domain, a big opportunity for the EU has emerged since the US system has started to show fallacies and shortcomings, both in terms of the protection of fundamental rights, and the sustainability of the competition and innovation model. This has generated the momentum for important EU initiatives such as GDPR, and also more recent actions such as those related to trustworthy AI. Given the many areas in which AI governance deficits might cause problems that gives the EU greater scope to act, from facial recognition to social credit scoring, the EU has an opportunity to lead the world on responsible AI development; similarly, the EU could also play a leading role on AI "for good", i.e. oriented towards the Sustainable Development Goals (Renda 2019; 2020). In this respect, the idea to invest on an ecosystem of excellence, along with an ecosystem of trust, appears appropriate but should be supported by adequate levels of investment in basic and applied research. In the domain of blockchain and DLTs, the rise of decentralised architectures described in the previous sections of this paper creates a new opportunity for Europe to propose an alternative model to the one dominated by US and Chinese tech giants. Indeed, Commissioner Thierry Breton has described the emergence of the edge/cloud architecture and the IoT as a unique opportunity for Europe to strengthen its global competitive position in digital technologies.

3.1.3. Cross-cutting dimension: credibility and trust

The credibility and trust dimension refers to the reputation and support the EU enjoys in a particular policy domain within and outside the EU. In this respect, the TRIGGER papers find a rather high degree of credibility, especially in the domain of open standards and open source software, whereas it is probably too early to judge whether the same occurs in AI and in blockchain or DLTs. The EU may however leverage its credibility built with the GDPR in those areas, especially if a significant investment in sustainable technologies and a consistent commitment to the "twin transition" will be effectively observed over time. At the same time, it is important to recall that EU's credibility, while reinforced by a long-standing commitment to "openness" and value-based policy, may be weakened by a more protectionist, less open stance by the "geopolitical" Commission.

The challenge now will be to continue promoting openness in a global context in which many countries are pushing for closed, intrusive, government-controlled technologies. If the EU would like to retain its reputation as a leader in the domain of OSS and open standards governance, it will have to ensure that open source code and open standards are incorporated in emerging key technologies.

3.2. Towards enhanced EU effectiveness in the digital domain: global challenges and long-term trends

The "geopolitical Commission" has raised significant expectations by making the "twin transition" its growth model, and even more by confirming its focus on sustainability and digital technology in the Next Generation EU plan, which is meant to transition the EU away from the dramatic impact of the COVID-19 pandemic. Raising EU actorness (and converting it into EU effectiveness) is going to be extremely challenging in this domain, identified by all the large superpowers as the key domain for world domination in the years to come: as a matter of fact, both Vladimir Putin and Xi Jinping recently observed that the country that will lead in AI will, as a consequence, come to dominate the world.

The analysis contained in the previous sections suggests that for Europe to increase its actorness and effectiveness in the domain of digital technology, effective, creative and forward-looking strategies will be needed both on the internal front, and in international cooperation and dialogue. Accordingly, Section 3.2.1 below outlines the contours of possible future EU actions in the domain of digital policy, whereas Section 3.2.2 explores the external dimension, by looking at the specific challenges of international cooperation and competition. Section 3.2.3 brings us a step forward by discussing the long-term scenarios identified in the TRIGGER project and deriving possible strategic priorities for the EU.

3.3. Challenges and emerging scenarios in global technology cooperation and governance

All the concerns raised as regards the role of regulators in the digital economy in the previous sections inevitably reverberate, with some degree of specificity, on the issue of International Regulatory Cooperation, on which the OECD has been leading the debate over the past years. For

example, the Trade Union Advisory Committee to the OECD (TUAC) recently called for "new rules for the digital transformation of the economy, including a 'BEPS II' Action Plan on taxation, an international agreement on data protection and algorithmic transparency, legal and ethical standards on Artificial Intelligence, and international cooperation to tackle corporate concentration and ensure workers' rights are upheld in the platform economy."[68] Already in 2015, the European Commission observed that "the digital economy also means that new types of trade barriers must be addressed", particularly for what concerns "the collection, storage, processing and transfer of data (including economic, financial, statistical and scientific information) and its digitalization", noting that "Regulatory cooperation, mutual recognition and harmonization of standards are the best tools to address the challenges of the digital economy"[69]. The recent APEC Ministerial Meeting in December 2018 also reiterated a call for "continued dialogue on relevant legislation and policies to promote transparency, regulatory cooperation and coherence in the digital economy", with specific emphasis on "policy and regulatory frameworks that protect privacy and consumer rights and promote interoperability in rules and regulations, whilst creating a favourable environment for the digital economy"[70].

Figure 5 below shows the OECD taxonomy of IRC mechanisms, which is helpful to locate where the challenges from the digital economy may lead the future of this crucial domain of regulatory policy. As a preliminary note, it is important to observe that the digital economy may have a variety of impacts on the IRC "universe": in particular, it may lead to specific challenges emerging in specific mechanisms, such as e.g. international standardization; but it can also have a "distributional impact" across mechanisms, leading to the increased use of specific mechanisms as opposed to others, for example due to specific problems in varying compliance with tight cooperation agreements. This may be due to some of the key features of the digital economy, which possibly hamper the quest for common or mutually agreeable solutions to the same problem.

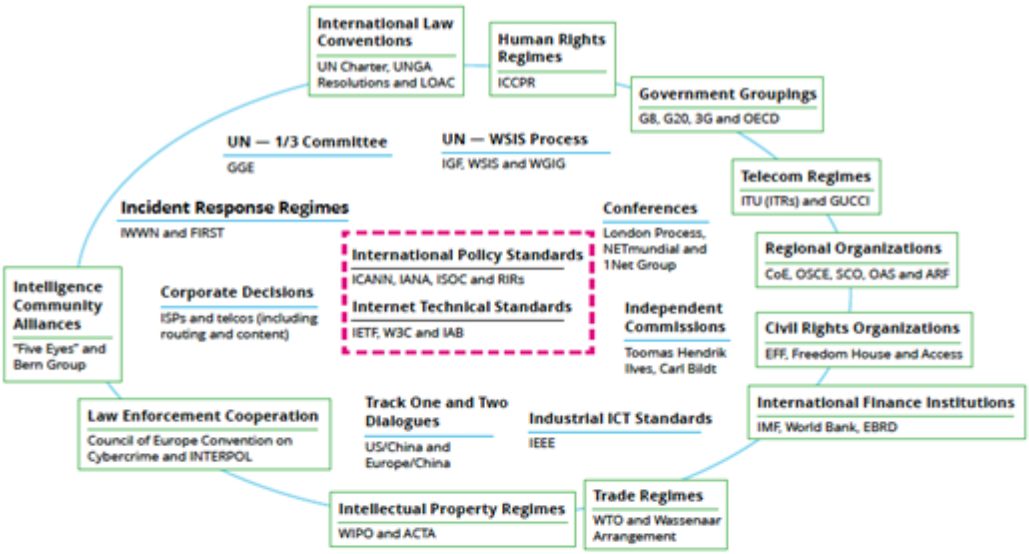
Figure 5. OECD Typology of International Regulatory Cooperation mechanisms

[68] https://tuac.org/wp-content/uploads/2018/05/1805t_GD-interim_TUAC-assesment_full.pdf
[69] https://ec.europa.eu/transparency/regdoc/rep/1/2015/EN/1-2015-497-EN-F1-1.PDF
[70] https://dfat.gov.au/trade/services-and-digital-trade/Documents/the-future-of-digital-trade-rules-discussion-paper.pdf

Source: International Regulatory Cooperation, Addressing Global Challenges, OECD (2013)

The Internet ecosystem consists of several layers of policy makers: globally through such UN agencies as its Department of Economic and Social Affairs (UN DESA), the United Nations Education and Scientific and Cultural Organization (UNESCO), the International Telecommunications Union (ITU), the World Health Organization (WHO), the United Nations Development Programme (UNDP), and the United Nations Office for Disaster Risk Reduction (UNISDR), and regionally through Regional Internet Registries (RIRs) such as the Asia Pacific Network Information Centre (APNIC), the Asia-Pacific Telecommunity (APT), Regional CERTs (Computer Emergency Response Teams); and individual countries' regulatory systems. Private sector actors, especially network operators, also play significant roles in the development of internet infrastructure and policy. The United Nations has convened a series of global meetings which have brought these actors together to make decisions on policy; and UN Agencies such as ITU have been instrumental in providing assistance in such areas as Universal Service/Access, Spectrum, Next Generation Network, among others. International Organizations such as Commonwealth Secretariat, OECD, EU, the International Organization for Standardization (ISO), the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF) and the Number Resource Organization (NRO) have also helped shaped key areas from a global policy level.

Figure 6. The complex landscape of Internet governance



Acronyms:

ACTA	Anti-Counterfeiting Trade Agreement	GUCCI	Global Undersea Communications Cable Infrastructure	IWWN	International Watch and Warning Network
ARF	Association of Southeast Asian Nations Regional Forum	IAB	Internet Architecture Board	OAS	Organization of American States
CoE	Council of Europe	IANA	Internet Assigned Numbers Authority	OECD	Organisation for Economic Co-operation and Development
DAC	Development Assistance Committee (OECD)	ICCPR	International Covenant on Civil and Political Rights	OSCE	Organization for Security and Co-operation in Europe
EBRD	European Bank for Reconstruction and Development	ICT	information and communications technology	RIRs	regional Internet registries
EFF	Electronic Frontier Foundation	ICT4D	Information and Communication Technologies for Development	SCO	Shanghai Cooperation Organisation
FIRST	Forum for Incident Response and Security Teams	IEEE	Institute of Electrical and Electronics Engineers	telcos	telecommunications company
"Five Eyes"	Alliance of Australia, Canada, New Zealand, the United Kingdom and the United States	IETF	Internet Engineering Task Force	UNGA	United Nations General Assembly
G8	Group of Eight	IGF	Internet Governance Forum	W3C	World Wide Web Consortium
G20	Group of Twenty	IMF	International Monetary Fund	WSIS	World Summit on the Information Society
GGE	Group of Governmental Experts (UN)	ISOC	Internet Society		
		ITRs	International Telecommunication Regulations		

Source: Nye (2014)

Against this background, IRC faces several challenges related to the trends exposed in the previous chapters. These are mostly related to context-specificity of digital policies, territoriality issues, enforcement liability rules and policy harmonization issues, and will be illustrated below following this taxonomy, as well as a "layered" approach, which echoes the description of the technology stack provided in Section 2.2 above.

3.3.1. The context-specificity of digital policies

Several challenges to IRC can follow from the different context existing in different legal systems. First, the different levels of penetration of digital infrastructure and connectivity in different countries may lead to different approaches and different impacts of similar policies in different countries. For example, an agreement on harmonizing eGovernment rules across countries may look very attractive to a country with strong connectivity and diffusion of eSkills in the administration, whereas other countries may face more fundamental obstacles to the diffusion of eGovernment in their administrations. One example is the still-voluntary and often complicated attempt, at the EU level, to implement the European Interoperability Framework, including the ISA2 programme to achieve interoperability between administrations: these problems are also exacerbated by legacy issues, such as the adoption of incompatible standards and very fragmented policy in the handling of data across administrations within the same legal system (Simonelli et al. forthcoming).

Second, and relatedly, the layered nature of the Internet ecosystem requires a holistic approach to Internet policy, which in turn determines the difficulty to identify "one-size-fits-all" solutions to individual problems. For example, the optimal solution to net neutrality may well differ in legal systems with facilities-based competition and relatively loose regulation at the infrastructure layer, as opposed to countries in which telecommunications networks are subject to network-sharing obligations, and most users rely on a single infrastructure (Bauer 2015). The less regulated and

competitive (in terms of number of competitors) the infrastructure layer is, the more mandatory net neutrality can become an appealing solution for regulators wishing to endorse open internet principles. Not surprisingly, the variety of international experience as regards infrastructure regulation has heavily affected the positions of countries trying to find a common solution to network neutrality in the past years.

Third, even without looking at geopolitical and strategic incentives (which will be done in the next section), legal systems differ significantly when it comes to their approach to the digital economy. A good example is the approach to data protection, which differs substantially in countries like the United States, where privacy is mostly considered a property right, and European countries, where privacy is considered as a fundamental right (Renda 2015). The reluctance shown by the European Commission over the past decade in recognising the US legal system as offering "equivalent protection" of privacy compared to the EU policy framework offers a good example of the problems faced by IRC in the field of privacy.

Fourth, it is common knowledge that the platformisation of the Internet has not led, so far, to the same impacts in all countries. The rise of superstar companies in the United States and China has not been paralleled by a similar development in Europe, where the approach to competition policy typically favours a more fragmented market structure. Regardless of the merits of the different approaches (see *i.a.* Renda and Yoo 2016), it is not surprising that the move towards regulating digital platforms has been stronger in Europe over the past decade, as opposed to the United States and China. This, in turn, made it very difficult to find common ground for exchanging practices and moving towards more stringent international cooperation between these blocs.

Fifth, and most notably, countries seem to be increasingly exhibiting diverging visions of the Internet economy and policy, as noted i.a. by O'Hara and Hall (2018), who identify as many as four Internets, including a US "commercial" internet, a EU "bourgeois" internet, a Chinese "authoritarian internet", and a more vulnerability-exploiting Internet (mostly in Russia, Iran and North Korea). This divergence, coupled with the increasingly strategic nature of the Internet for global competition, leads to a deteriorating climate for IRC in various aspects of Internet governance. Good examples are again network neutrality, and fake news/disinformation. Both debates have evolved into discussions on how to ensure that the Internet remains open, and an enabler of free speech: the view of countries around the world does not seem to be fully aligned on these issues.

Finally, these diverging views are also echoed in end users' preference for specific policy priorities, such as protecting end user privacy. Graf et al. (2016) show selected results for all countries based on a sample of 15,000 respondents (1,000 in each country, margin of error 3.1%), and finds relative similarity of consumer preferences in most European countries, the United States, Canada, Australia and New Zealand. In contrast, the authors observe most of the developing world, with consumers in India, the Middle East, Russia and Mexico, much more willing to trade their privacy for the convenience that the internet and cloud can bring. While we can expect fluctuations in perceptions across the board, particularly due to domestic political developments, the data indicate that the greatest demand for privacy solutions will originate from the most advanced economies: the EU, Canada, Australia/New Zealand, and the United States.

3.3.2. Trust between governments: the rise of cybersecurity, protectionism and "data sovereignty" stances

Apart from differences in national contexts that may affect IRC, perhaps the most evident barrier to regulatory cooperation is the increased evidence of lack of trust among governments when dealing with the Internet and the digital economy. There are several reasons for this emerging lack of trust, which can be added to the already-mentioned divergence in overall domestic approaches to Internet policy.

First, the challenges created by the digital economy for domestic regulation lead to a weakening of government commitments at the international level. For example, governments can commit to enforcing copyright domestically, but (as already mentioned in Section 1) technology has always been able to escape from the attempts of national regulators to curb copyright infringement (Renda 2011). Similarly, network neutrality cooperation among countries faces the limit of enforcement (i.e. how to ensure that specialized services do not excessively disrupt the open, best effort Internet); as well as the fact that mandatory network neutrality is unlikely to make the Internet any neutral (Renda 2014). In many areas, delegated enforcement leads to lack of control on the impacts of public policy, creating significant uncertainty for regulators. Furthermore, the existence and evolution of the Deep and Dark Web make it difficult for governments to both commit to regulatory outcomes and trust their counterparties' commitment towards at least trying to pursue common principles. In this respect, trust is also undermined by difficulties in cooperating in cybersecurity, a field in which attribution of cyber-attacks is extremely difficult, and state-sponsored attacks are thought to be as frequent as they are constantly evolving (Griffiths *et al.* 2018).

Against this background, the fact that Internet governance has remained under the strong influence of the United States since the outset has been met with criticism from other parts of the world, potentially further undermining trust among parties at the IRC table. International bodies have called for responsibility for the internet to be transferred to more international arenas: for example, as recalled by O'Hara and Hall (2018), the Working Group on Internet Governance, under the auspices of the ITU recommended already in 2005) that the United States relinquish oversight of the system: at the same time, the tendency in this debate is to propose alternative forms of Internet governance that would strengthen government control, potentially to the detriment of multi-stakeholder dialogue and civil society participation. Singer and Friedman (2014) describe a growing competition to regulate the Internet between the ISOC, the ITU and 27 individual countries, in which the ISOC is viewed by many countries as being too closely aligned with the large internet providers and with U.S. interests.

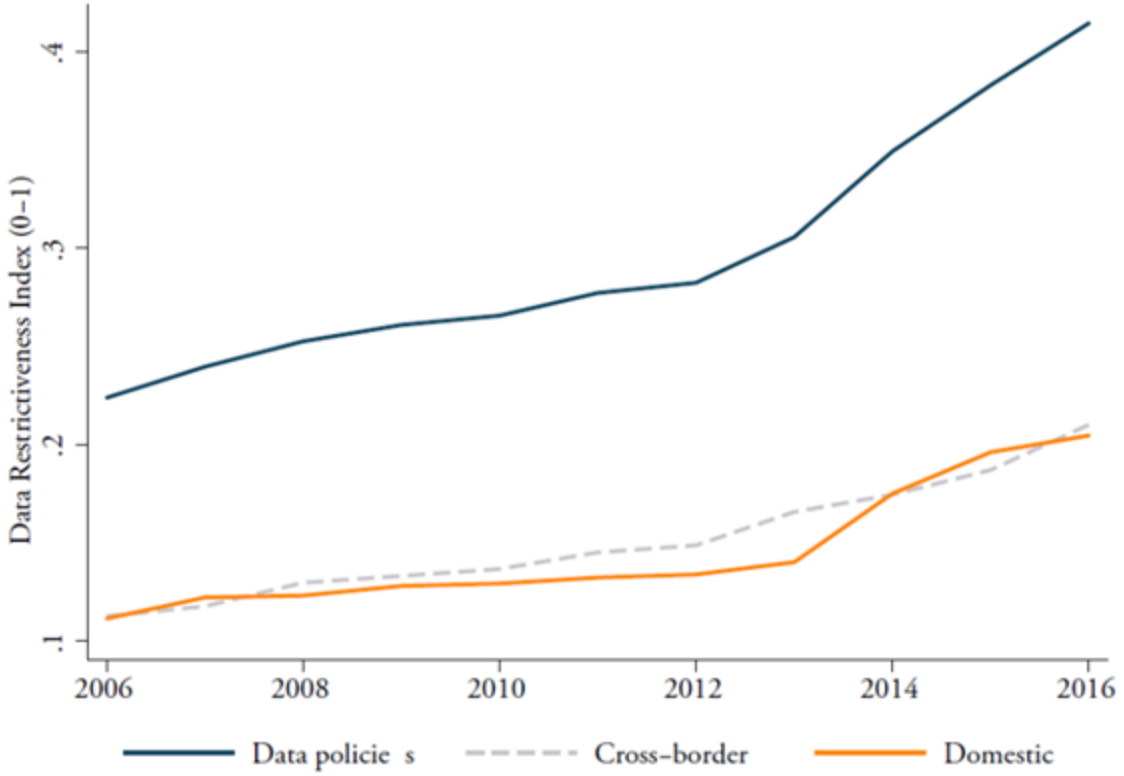
Moreover, several scholars have documented a rise of digital protectionism over the past decade, including (especially after the Snowden revelations[71]) data localisation requirements[72]. This is extremely costly for the global economy, if one considers that the contribution of data flows to global GDP is already thought to be bigger than the contribution of the flows of goods (Manyika *et al.*, 2016). Figure 7 below shows the evolution of the Digital trade Restrictiveness Index calculated by ECIPE, as described in Ferracane et al. (2018). The authors conclude that lifting these

[71] Edward Snowden revealed information detailing the extent of the U.S. National Security Agency's (NSA) activities. For EU privacy advocates, they constituted a "proof" that EU personal data stored by U.S. internet and mobile service providers did not offer the equivalent protection as data stored within the EU.

[72] Digital protectionism goes way beyond data protection, covering localization requirements of computer installations, disclosure of computer source codes (computer operating systems) or the discriminatory treatment of digital products (music, video, software, e-books) transmitted electronically. Commercial flows of goods can be impacted by restrictions on data from the moment products include services, software and other connectivity applications (embedded goods).

restrictions would generate a TFP increase of about 4.5 percent across countries, with stronger benefits in data-intensive sectors such as retail and information services. Aronson (2018) argues that it will not be easy to set international rules to limit digital protectionism without shared norms and definitions. This is however complicated by the fact that the US, EU, and Canada have labelled other countries policies' protectionist, yet their arguments and actions sometimes appeared unconvincing and biased, and China still fails to follow key internet governance norms by using a wide range of hostile cyber strategies to "censor information flows and impede online market access beyond its borders".

Figure 7. Evolution of the Digital Trade Restrictiveness Index, 2006-2017



Source: ECIPE Digital Trade Restrictiveness (DTRI), Ferracane *et al.* (2018b). The index varies between 0 (completely open) and 1 (virtually restricted) with higher levels indicating increasing levels of data restrictiveness. * The index covers 64 countries around the world representing more than 95 percent of value-added content of gross exports.

In a study on prospects for cloud computing for RAND, Graf et al. (2016) find that "there are significant market forces which may drive cloud services and the internet infrastructure towards increased data localization" in the future, and "anticipate that the combination of technical need, consumer privacy concerns, state security concerns and corporate confidentiality needs will lead to an increased demand for contractual and technical mechanisms to ensure that data is kept within specific geographic and/or national boundaries"[73].

These developments, coupled with the growing strategic important of retaining control of the Internet infrastructure and the flow of data, ultimately led many countries to consider forms of "data sovereignty" policies. Perhaps the most famous example is the EU GDPR, which is designed to apply beyond the EU borders, whenever the personally identifiable data of European citizens are

[73] https://www.rand.org/content/dam/rand/pubs/working_papers/WR1100/WR1144/RAND_WR1144.pdf

being processed. These policies often face the problem of territoriality and the "as a service" provision of many digital products, coupled with cloud storage.

Finally, a look at the emerging national strategies for AI and data-driven innovation also casts a dark shadow on the prospect for enhanced IRC in the Internet space over the coming years. Many countries are indeed discovering the enormous strategic importance of controlling the infrastructure, the data and the computing capacity related to the new technology stack. Notable examples are the *querelle* over the possible ban of Huawei from the deployment of 5G networks in the United States and beyond; Europe's reported temptation to build its own European microprocessors and calls to launch an "Airbus for AI" as a form of industrial policy; and the European idea of building "data spaces", which may evolve towards orchestrated ways to build European champions in key sectors such as automotive, healthcare, etc. Looming on this debate is also the growing competition between countries in securing advantage in new technologies such as quantum computing and cryptography (Gros et al. 2018); and the increased threat to national security represented by the expected boom in the Internet of Things over the next few years, which will expand the possible "attack surface", thereby requiring enhanced control over data flows and ultimately, a likely deviation from internet openness principles.

3.3.3. Trans-national private regulation: keeping regulators at bay

As a corollary to what was already explained with respect to difficulties of enforcement, it is important to observe that the digital economy exacerbates a growing trend in global governance, i.e. the rise and prominence of private governance. On the one hand, the institutions governing the Internet, such as ICANN and the IETF, are private and come from a tradition of very loose checks and balance when taking decisions. On the other hand, the rise of global platforms serving billions of customers in many countries has come with a degree of self-regulation. Already in 2011, Tim Büthe and Walter Mattli classified Windows API as a form of private regulation. Today, companies like Facebook, Google, Amazon, Uber bring their governance across borders, *de facto* regulating through contract transaction the way in which large portions of their markets work. This is a reflection of what happened in other sectors over the past decades: standards like GlobalGAP or the Marine Stewardship Council have become key elements in the governance of value chains around the world, and very often provide an alternative to sometimes less predictable applications of the rule of law in many countries (Cafaggi and Renda 2012); similarly, the contracts applied by large platforms to their businesses are standardized and largely independent of the national boundaries, which obviously streamlines governance for these players, but at the same time can create frictions with national legislation. This tendency is likely to be amplified by technological evolution. Large IoT networks, for example, and the use of smart contracts know no legal borders but rely on code to execute functions and solve tensions and controversies.

The tendency towards the rise of trans-national private regulation in the digital economy is now being met with some resistance, as explained above, as some legal systems (mostly European) place increased pressure of large technology companies to comply with national law. The tensions emerging between so-called GAFA (Google, Amazon, Facebook, Apple) and the European Commission on respecting consumer and competition rules, enforcing data protection and the right to be forgotten and tackling disinformation in view of the upcoming political elections are only one out of a series of episodes that point in this direction[74].

[74] https://www.bbc.com/news/technology-45519506

Finally, trans-national private governance is poised to create new challenges for policymakers in the years to come, as the spread of more sophisticated malware and "deep fakes", coupled with increase calls for protecting privacy and freedom of expression, may create a "trilemma" for large giants: encrypting communications to protect user privacy and respond to widespread calls for enhance protection of personally identifiable data may weaken the control of disinformation, and the use of alternative means to tackle disinformation might in turn lead to taking down content to the detriment of freedom of expression[75]. Governments may need to equip themselves to be able to address this upcoming set of challenges, in particular by developing ways to use technology to protect end users.

3.3.4. Territoriality, liability and fragmentation: emerging challenges for international regulatory cooperation

Looking at IRC more closely, the main challenges resulting from the rise of the digital economy can be subsumed under three main categories: territoriality issues, which represent the mirror image of the prevalence of trans-national private governance in this domain; liability issues, due to difficulties in apportioning and attributing responsibility for damage caused by technology to end users; and the increasing fragmentation of the legal environment.

3.3.4.1 Territoriality and the digital economy

Law is linked to territory, whereas digital platforms operate across (almost all) borders. While the global features of the open Internet have created enormous value to users around the world, they also have inevitably led large companies in a situation in which they could engage in some degree of "forum shopping" when it came to the establishment of their headquarters, their internal tax policy, and their policy for data protection. The rise of cloud computing, which allows for remote access to data, software and even hardware capabilities from any location around the world has further amplified this phenomenon: data servers and storage centres can be located anywhere around the world, and be subject to the legislation of the country of choice. This, in turn, might lead to both a "race to the top" (i.e. companies will try to locate their data centres in the safest, best governed locations); but also a "race to the bottom" (i.e. digital companies could opt for more "generous" locations when it comes to data protection).

The reaction of many governments over the past years has gone in the direction of strengthening extra-territorial effects of their most important laws, sometimes in inconsistent directions. For example, the US 2018 CLOUD Act implies that US law enforcement can demand data and emails to be handed over if stored by a US company, regardless of where in the world the data is stored. On the contrary, the EU GDPR places individual privacy rights at the forefront, requiring that all data related to EU citizens be subject to its provisions regardless of where the company is headquartered and where the data are kept: based on GDPR, data stored on citizens must be either stored in the EU so it is subject to European privacy laws, or within a jurisdiction that has similar levels of protection. The extra-territorial impact of the GDPR has been given extensive and generous interpretation by the courts and data protection authorities, as recently confirmed by the European Data Protection Supervisor in its guidelines on the territorial scope of GDPR[76].

The Internet society has recently stigmatized the rise of extra-territoriality in digital policy, by denouncing the unintended consequences of recent interventions such as the CLOUD Act and

[75] https://www.politico.eu/article/mark-zuckerberg-facebook-privacy-encryption-whatsapp-fake-news-misinformation
[76] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf

the GDPR, but also the 2014 Court decision in *Google Spain*, the 2017 Supreme Court of Canada decision to uphold orders for Google to "de-index" a website, asserting the jurisdiction of Canada's courts over Internet intermediaries in other countries; the US decision to block sci-hub in 2017, in addition to the seizure of its domain names; the Chinese move to increase the extra-territorial reach of its content monitoring and filtering regime; and recent trends towards replacing 'notice and takedown' approaches towards a positive obligation for technology platforms to police existing content or even prevent it from being uploaded. Table 1 below illustrates the perceived risks of extra-territoriality in national legislation.

Needless to say, the extra-territorial effects of domestic legislation require a degree of cooperation between national authorities in the enforcement of the rules, a need which the growing lack of trust described in the previous sections does not help to satisfy. This is further amplified by the fact that states regularly carry out cyber-operations in foreign territory: among others, Watts and Richard (2018) observe "by means of its interconnected framework, cyberspace presents States unprecedented access to information and objects on the territory of other States".

Other issues that emerge due to the complex interplay between national legislation and private governance of multi-national corporations are the following:

- On taxation, due to the specific features of the Internet, large companies have been able to use both transfer pricing and strategic location to minimise their tax exposure, leading to a mismatch between the place where value is created, and the place where taxes are paid (OECD 2018). This has led some countries to start envisaging forms of "web taxes", based on the companies' turnover in the country where value is created.
- In some circumstances, internet companies artificially limit the ability of end users to access cross-border websites and services by engaging in geo-blocking and market partitioning. While these practices do not always have a negative impact on the market and can also amount to welfare-enhancing practices or be needed to comply with the law, in some cases they are meant to maximise the company profits by limiting cross-border access. McDonald et al. (2018) report the first wide-scale measurement study of geo-blocking, mapping capabilities offered by large CDNs and cloud providers, and find that geo-blocking occurs across in nearly all of the 177 countries studied[77].

Table 1 - Internet invariants and externalities of extra-territoriality

[77] https://censoredplanet.org/assets/403forbidden.pdf

Internet Invariants	Externalities of Extra-Territorial Jurisdiction
***Global reach and integrity**:* An 'end to end' Internet where information sent from any point can get to any other in any network around the world. **Accessibility**: Anyone can use the Internet, not just to consume but to contribute content, put up a server and attach new networks.	**Internet fragmentation**: negates and challenges the global reach and integrity of the Internet; creates new digital divides where access to information and communication tools is uneven.
General purpose: The Internet is not designed for specific purposes or business models, but for general use. **Reusable building blocks**: Technologies may be deployed for one purpose, but used later or by others to do something new. **No permanent favourites**: Success depends on relevance and utility, not on special status. It must not be 'locked in' by today's winners. **Permission-less innovation**: Anyone can set up a new service on the Internet without having to ask permission, as long as it meets existing technical standards and best practices.	**Inconsistency** - Different stakeholders try to enact decisions and complicated rules that are often not easily enforceable. With a proliferation of rules and complexity, the largest organizations can most easily comply, creating competition issues for smaller firms and even a **new digital divide** between large and established companies, and smaller, potentially more innovative ones. Vertically integrated solutions driven by the legal and cultural backgrounds of the biggest players and countries are favoured, instead of open, reusable technologies that can be repurposed by new players. Instead of being distributed around the world, the benefits of the Internet are increasingly concentrated in the countries with the most international influence and the companies with the resources to comply, turning certain companies into *permanent favourites*.
Interoperability and mutual agreement: through open technology standards and mutual agreements between operators of different parts of the Internet. **Collaboration**: The best solutions to new issues come from willing collaboration between stakeholders.	**Power-grabs** – States try to grab or reassert power at the international stage, as each races to come out on top, imposing unilateral interests in a top-down, closed way. This intensifies both jurisdictional conflicts and friction between networks. **Uncoordinated action** - Unilateral top-down actions displace and undermine collaborative ways of examining issues. They can negatively affect the development of the network. Because the Internet is a network of networks, if changes are imposed on different networks there is a risk that those networks stop working together. This pulls stakeholders apart instead of bringing them together, resulting in a 'zero-sum game' world where everyone is a loser.

Source: ISOC (2018)

3.3.4.2 Cybersecurity and liability across borders

In cyberspace, regulatory cooperation is essential to promoting security, which in turn underpins all international activities, from data transfers to trade. There can be no smooth functioning of ICT without cybersecurity and the protection of critical information infrastructure. In the past few years, the "attack surface" has expanded exponentially along various dimensions, such as the terrain in need of defence, the proliferation of digital attacks, and notable changes in the attack vectors being used. The number of reported vulnerabilities is also growing. In its 2018 Internet Security Threat Report,[78] Symantec reported that it witnessed a 13% increase relative to the previous year in overall reported vulnerabilities in 2017 and, even more concerning from a critical infrastructure perspective, a 29% increase in reports for industrial control systems, in addition to a 92% increase in downloader variants of malware, a 54% increase in variants of mobile malware, a 46% increase in ransomware variants and a 600% increase in IoT attacks compared to the rates observed in 2016 (Griffith et al. 2018).

In addition to the technical evolution and characterisations of digital threats more broadly, one area of central concern is the ongoing "weaponization" of this domain for strategic purposes by state and non-state actors. Given the range of politically motivated, state-sponsored attacks, 2016-17 notably represented an important inflection point for cybersecurity as a domain of strategic activity. We witnessed the widespread and indiscriminate targeting of civilians (*WannaCry*); targeting of civilian critical infrastructure (*NotPetya*); and the targeting of democratic processes through the acquisition and release of sensitive information from specific electoral campaigns (the 2017 French presidential elections), the general public and political elites through information operations leveraging social media (the 2016 US presidential elections), and the electoral infrastructure itself through results reporting platforms (the 2016 Ghanaian presidential elections).

As a result of this militarisation and potential for escalatory conflict, governments have recognised the need to address cyber conflict and have done so through a number of multilateral and multi-stakeholder fora. In 2016, the Organization for Security and Co-operation in Europe adopted an enhanced list of "confidence-building measures" to enhance security and stability in the cyber domain. In 2017, the G7 published a declaration recognising the urgent need to establish international norms for responsible nation-state behaviour in cyberspace. To date, the primary mechanism has been the UN Group of Governmental Experts (UNGGE), which has focused on non-binding normative agreements of expected state behaviour. In June 2017, the group failed to come to an agreement on core aspects related to government behaviour, particularly around the applicability of international law in cyberspace. The lack of progress in implementing agreed-upon cyber norms has enabled the continued militarisation of cyberspace. While many governments agree that international law exists and extends to behaviour in cyberspace, questions remain on how it applies in practice. The issue, therefore, is not a lack of potential legal or normative frameworks but rather in the lack of consistent implementation of existing frameworks.

Traditional dissatisfaction for the lack of international rules aimed at and capable of striking a balance between the potentially clashing interests of global trade, on the one hand, and national rules aiming at ensuring cybersecurity, on the other hand, mainly arose because the WTO agreements (including GATS and TRIPS) are largely considered inadequate to deal with the manifold and complex issues arising from the modern-day digital economy, if only due to the fact that they were adopted more than twenty years ago. A possible response to the rising temptation of a unilateral approach to cybersecurity seems to rely on the interaction between international standardization and the existing WTO legal framework, which could try to reaffirm its centrality

[78] "Internet Security Threat Report" Symantec. Volume 23.

with particular reference to digital trade issues. In particular the practice within the TBT Committee shows that WTO law could still be the proper framework in which States may seek harmonization of technical standards related to cybersecurity issues.[79]

As already mentioned throughout this section of the report, the key obstacle to reaching a suitable level of cooperation is trust, and the latter is critically undermined by the difficulty in attributing liability and responsibility in cyberspace, due to the ease with which practices and chains of actions can be hidden or obfuscated. Various techniques exist in cyberspace, which can lead to masking state-sponsored attacks; and techniques such as "onion routing" successfully hide the origin and purpose of specific file transfers (Mathakar et al. 2017). Against this background, International regulatory Cooperation suffers from a lack of certainty and rising fragmentation. A recent report by the Swedish National Board of Trade (2018) highlights this issue by observing how "the various regulatory paths that have been developed in the past to address IT security regulation stem from and are based on national needs and concerns to protect critical infrastructure, rather than a strong interest in free trade and international harmonization", and that "these premises can make it extremely burdensome to find internationally accepted, standardised regulatory principles and solutions for international IT security regulation"[80].

The international standard that provides the technical platform for cybersecurity certification is called Common Criteria (CC). This standard is used as the basis for government driven certification schemes and because certifications are typically conducted for the use of public agencies and critical infrastructure. The standard is supported by a Common Methodology for Information Technology Security Evaluation (CEM), which describes how the evaluation should be carried out, using the criteria and evaluation evidence defined in the standard. To create trust and to enable opportunities to ensure that assessments are made in an equivalent manner, so called Protection Profiles (PP) and Supporting Documents are used and are adapted to specific technical areas. PP are documents used as part of the certification process according to ISO/IEC 15408 and the CC. Collaborative Protection Profiles (cPP) following the standard are developed in international Technical Committees (iTCs); this process follows international principles of openness and transparency in standardisation. Supporting Documents have been developed both on the regional (SOG-IS MRA) and international (CCRA) level for specific product types, i.e., additional requirements for specific product types and technologies[81]. What should be observed, however, is that the development of Supporting Documents does not (compared to PP) always occur through an open process. However, Supporting Documents are still mandatory to use in many cases in order for a supplier to obtain a certificate. Again due to lack of trust, as well as national security concerns, individual countries do not necessarily share the structures and practices that will be used for cyber evaluation. Consequently, it has been difficult to generate more uniform regulatory schemes for IT security certification internationally, and certification according to the CC is an expensive and lengthy process.

3.3.4.3 Fragmentation: avoiding the "race to the bottom" in emerging fields of digital policy

Fragmentation is a widespread problem in cyberspace, hampering IRC in many respects. Recent areas in which divergence of interests and lack of sufficient regulatory cooperation include artificial

---

79 http://www.qil-qdi.org/digital-standardization-cybersecurity-issues-international-trade-law-forthcoming/#_ftn70

80 https://www.kommers.se/Documents/dokumentarkiv/publikationer/2018/The-Cyber-Effect.pdf

81 The two systems provide for different levels of insight and transparency as well as different possibilities for various countries to participate and affect regulation.

intelligence, the international law on autonomous weapons, policies towards blockchain, 5G communications and the IoT.

On Artificial Intelligence, China is on its way to becoming the most powerful global economy, with the United States currently stepping back from the proactive, almost uncontested leadership that they have enjoyed over the past decades. This is reflected in many domains of global governance, including climate policy, trade policy, and to some extent even the G7/G20. The international political order will be affected heavily by this transition. In particular, it is reasonable to expect that due to the data-hungry nature of current AI applications (mostly based on machine learning), and the pervasive nature of such applications, the emerging technology stack (figure 1 above) will be considered as "critical infrastructure", i.e. essential to national stability in the near future, most likely within the next ten years in many developed countries. The explosion of the Internet of Things and the massive generation of data-driven, AI-powered applications that run key critical infrastructure such as energy grids, Internet pipelines, the food chain, the ATM network, hospital logistics and care delivery will gradually lead countries to try to protect the IT stack as a domestic asset.

The risk of foreign "intrusion" into the data architecture, already existing today (suffice it to think about the Russian meddling in US elections), will gradually become an existential risk for governments. Thus, a temptation to invoke so-called "AI sovereignty" or "AI autarchy" may emerge, just like sovereignty-related sentiments and reactions were elicited by the Snowden revelation related to NSA mass surveillance, especially in countries like Germany and France; and the threat of Russian or Chinese meddling into elections triggered reactions in the U.S., Italy, the UK and also recently in Australia[82]. "AI sovereignty" will be even more loudly invoked in the age of quantum supremacy, given the need to avoid that advances in cryptography provide hostile nations with important strategic advantages in global intelligence. Despite the inherently global nature of technologies like the Internet and AI, such tendency may emerge both in non-democratic countries, and in democratic ones.

The most obvious response to this potential trend would be to develop deeper cooperation on the relationship between AI and international human rights. In this respect, the Toronto declaration prepared by Amnesty international and Access Now proposed a framework for reconciling AI development with the International Human Rights framework. However, despite alarming findings on the misuse of AI and, more generally, big data analytics as "weapons of math destruction" (O'Neil 2016), or as tools liable to "automate inequality" and exacerbate lack of accessibility; and despite the mounting evidence of use of AI systems to manipulate public opinion and meddle through domestic elections, let alone score and rank citizens based on very intrusive personal data mining, the global community does not seem likely to reach an agreement on minimum standards of responsible use of AI: the stakes are simply too high. This also implies that autonomous weapons, cyberwarfare and possible negative effects of AI on jobs, social equality and cohesion, and the environment may not be subject to a global governance effort in the next few years.

A different angle to the interface between global governance and AI, which might hold more promise in the international community, is the incorporation of AI in the overall discussion on the Sustainable Development Goals. This approach, represented in ongoing initiatives such as ITU's "AI for Good Global Summit", focuses on the uses of AI that can help the global community achieve the SDGs. This focus was also shared and echoed by several large private companies and

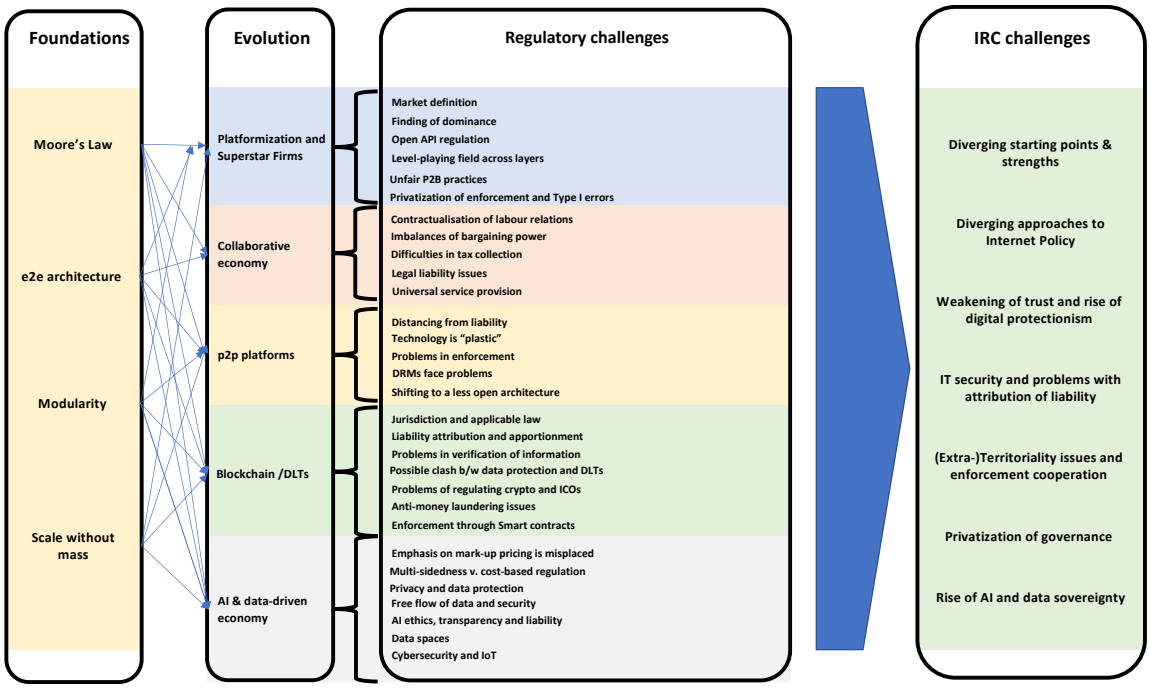
[82] See i.a. Hamilton, C., Australia's Fight Against Chinese Political Interference, Foreign Affairs, 26 July 2018.

foundations, which profess their commitment to achieving the 2030 goals through enhanced use of AI. However, looking at current trends such as the resurgence of nationalism in politics, deteriorating rule of law in some European countries, new protectionist stances and tariff wars in trade, short-termism in social policy and reiterated denial on climate change, the agreement reached in September 2015 by 193 countries on the SDGs seems to belong to a very distant era in human history. Indeed, today the United States have reached a record low in its commitment to SDGs, Brazil is entering a new era of populism and China struggles to show leadership on environmental, and even more social, achievements. Recent reports confirmed that, with the exception of Scandinavian countries, all high-income countries are far from a trajectory that would lead them to achieve the 17 SDGs, and struggle in particular with four objectives related to sustainable consumption and production patterns, climate action, aquatic life and life on land[83]. In general, the current landscape seems to highlight the existence of a huge gap in leadership in AI global governance: a gap that the U.S. and China are probably unwilling to deal with, and that only the European Union, if acting together, might have the strength to fill.

3.3.5. Mapping regulatory challenges and outlining possible solutions

Figure 8 show a synopsis of this analysis by summarizing the links between features, trends and challenges.

Figure 8 - Mapping the key challenges for regulation and IRC from the digital economy



Source: Author's elaboration

More in detail, the platformisation of the Internet ecosystem and the rise of Superstar firms are mostly due to the network externalities coupled with the modularity (or "layered architecture") of the ecosystem and with the digitization of information goods, which results in the possibility of achieving scale without mass in a context in which competition is winner-take-all. The rise of the

[83] https://www.un.org/sustainabledevelopment/sustainable-development-goals/

collaborative economy is even more linked than that of large platforms to the end-to-end nature of the Internet ecosystem and is nurtured almost exclusively by a combination of direct and indirect network externalities, coupled with increasingly sophisticated algorithms. Complexity is on the rise in the Internet ecosystem, as some of the most powerful platforms (Netflix, Uber, Airbnb) could succeed in the market thanks for a previous generation of (mostly mobile) platformisation, with the rise of the smartphone and the almost-duopoly between Android and iOS. Similarly, as shown in Figure 3 above, blockchain and DLTs rely on the IP protocol and feature the possibility of launching decentralized applications that ultimately constitute a deviation from the open internet and/or large platforms. The rise of AI as a pervasive, general-purpose technology and widespread, unprecedented data availability contribute to emerging trends. As a matter of fact, these trends are complementary, rather than alternative, and contribute to varying degrees to posing challenges for regulators.

For example, platformisation coupled with the rise of Superstar firms created problems in competition policy, with market definition and the finding of dominance increasingly challenged by the winner-take-all nature of "Schumpeterian" competition in many of these markets, and the need to impose full interoperability with established, vertically integrated solution as an emerging and controversial solution to the growing power of these players (the public policy approach to "open API", as a matter of fact, was born with the EU Microsoft case on client-server interoperability). The platformisation of the Internet ecosystem also leads to problems of cross-layer competition (as in network neutrality, but also grid neutrality, and in competition between collaborative economy and established businesses such as taxis, or hotels), and of unfair and obscure practices applied by platforms to the businesses they host, irrespectively of the existence of a contract between them (so-called P2B unfair practices). Platformisation also led in some jurisdictions to an increased demonization of certain platforms (especially for what concerns privacy and hate speech) and an ever-growing delegation of enforcement powers in their same hands (for example, in the prosecution of hate speech and copyright infringement, but also cybersecurity).

The collaborative economy has created well-known challenges for regulators, in addition to the already-mentioned competition ones, the disintermediation of labour relations and the imbalances of bargaining power (especially in the case of crowd-workers) have been accompanied by problems in tax collection, displacement of liability and problems in the provision of universally accessible services due to lack of specific responsibility, as well as problems related to the overall privatisation of employer-employee (or microenterprise) relations.

Regulators have already faced almost insurmountable problems when facing p2p platforms, especially in the copyright sphere, but also when dealing with blockchain as a specific sub-case of p2p technologies coupled with consensus algorithms and distributed ledgers. The dis-intermediation and autonomous organization features of these platforms are such that the law, most often, is perceived as a non-autochthonous element of these ecosystems. Problems in attributing liability, verifying and certifying transactions on the ledger, plus the need to reconcile these technologies with key domains of legislation such as data protection, fundamental rights and cybersecurity create a significant space for regulatory reform and agile governance in the coming years. The case of smart contracts, among all, is perhaps the most difficult to handle for regulators, given the inevitable ambiguity of regulating controversies through code (Grimmelman 2019).

Finally, AI and data-driven innovation exacerbate most of these problems, at the same time creating new ones, such as the need for well-defined ethical boundaries and principles, and to operationalise those principles in a way that promotes the alignment of these very powerful technologies with

social welfare and other government goals, such as fundamental rights, well-being and/or sustainable development (Renda 2019).

The described regulatory challenges are non-exhaustive and obviously co-existing in many circumstances, and spread throughout the regulatory governance cycle as normally defined by the OECD. In particular, the digital economy critically affects the design of regulations, imposing an adaptation towards more principles-based, or outcome-based policymaking rather than very prescriptive, detailed policies. Similarly, the digital economy has brought a wave of privatization of regulatory design, implementation and enforcement, bringing entire areas of public policy or administrative law under the aegis of contract law, and often across borders. At the same time, the digital economy has already determined the rise of experimental, adaptive approaches to policymaking such as regulatory sandboxes or randomized controlled trials, or more simply co-regulatory schemes based on periodic reviews of regulation and relative flexibility in implementing reforms over time. The digital economy also leads to massive changes in enforcement: so far often privatized and delegated to technology such as algorithms or digital right management systems, enforcement is today substantially veering towards RegTech and SupTech solutions, in which regulators show to have finally awaken to the use of technology to regulate technology. Regulators increasingly look at nuanced approach to data, such as data-sharing arrangements and the treatment of data hoarding as a competition problem, leading to mandatory data sharing obligations. The first examples of propose treatment of data as labour are also interesting and will trigger debate in the months to come.

Importantly, the domain of International Regulatory Cooperation is heavily affected by these features of the digital economy, and also more indirectly by the limited trust and diverging interests that these same features determine when looking at OECD countries. While a degree of cooperation exists, existing superpowers often move mutual accusations and display completely different starting points at the negotiation table. The imperative in the coming months and years will be to work towards the identification of common rules and principles for the new technology stack, around which to work towards. A prosperous future, in which new technologies can help OECD countries achieve sustainable growth. This will require, among others, exchange of practices on data and AI policy, cooperation on experimental and adaptive policymaking, common and solid standards on IT security and data privacy, and regulatory cooperation in the enforcement of (hopefully) more harmonized domestic rules on privacy and data protection. This will, *i.a.* help resist the temptation of digital protectionism, at the same time leading OECD countries towards gains in GDP and progress towards well-being and sustainable development

3.4. One step further: long-term scenarios and EU actorness

The choices that Europe and other large powers will make in the coming months as regards its digital agenda are likely to exert a significant impact on global trends. At the same time, identifying such trends and possible scenarios is also important to assess and predict the possible effectiveness of the EU in the domain of digital policies in the years to come. As things stand, for example, there seems to be a non-insignificant possibility that global superpowers will not reach a suitable agreement on the governance of common internet resources, and eventually promote a "splinternet", i.e the forking of protocols and specification that current maintain the global nature of the Web. This is already visible both in terms of technological rivalry (e.g. over 5G), and

also when it comes to the looming competition in developing and emerging economies between China's Digital Silk Road and "Western" standards.

TRIGGER is developing long-term scenarios based on the interplay between different megatrends, and in particular based on different degrees of EU strength and global governance cohesion. The resulting scenarios, and their consequences for EU digital policy, are defined below.

- In a **"duplomacy"** scenario, by the year 2050 the geopolitical landscape has divided into four power blocs organised primarily around access to various resources – energy, human skills, water, and arable land. Multilateral cooperation between blocs is sparse, temporary, and insufficient to address global scale problem areas (e.g. climate change, financial/economic crises, pandemics etc.). The EU remains a strong power, albeit in a fragmented global governance. One of the underlying assumptions is that the tensions generated by competition between different blocks and the tendencies towards strategic autonomy lead powers to ring-fence, adopting own standards and holding tight to their critical infrastructure. In this scenario, the EU gradually strengthens its digital policy, raising the standards to make the digital age fit for Europe, rather than the other way around. The peril of competition from products and services from non-EU countries leads to a resurgence of protectionism and an exacerbation of the rhetoric on digital sovereignty. The transition towards a distributed economy leads the EU to gradually reserve the edge/IoT layer and the cloud federation to European products, and compliant products from Europe's own "bloc". The fragmentation in R&D and standards development slows down, inevitably, the pace of progress: depending on the extent and direction of competition between blocs, technological development is not necessarily oriented towards global public goods, which in turn threatens mankind's ability to pursue common objectives. At the same time, the core of economic activity shifts towards the largest blocs (e.g. Asia), which may lead Europe to partner with Africa to rebalance its demography and increase its weight in the global competition between blocs. In such a scenario, the EU consolidates the digital policy shaped by the Juncker and even more the von der Leyen Commission: international collaboration and dialogue activities are reduced, and the future data spaces and cloud federation are gradually accompanied by a strongly governed IoT/edge strategy, aimed at securing the reliability, resilience and trustworthiness of the technology stack. There is little or no cooperation on cybersecurity, and this lead the "duplos" to further ring-fence in the age of extended reality, by adopting policies that leave no space for foreign intrusion in the form of deep fakes.
- When fragmented global governance is coupled with a weak Europe, in the so-called **World Wide Gap scenario**, the result is a worst-case one for the EU. In such a scenario, no significant global cooperation schemes survive, and the EU itself is prey of a tendency towards the fragmentation of governance. In this scenario increases in economic inequalities radically undermine efforts in global governance, and exacerbate social, political, and infrastructural gaps around the world. Trust in international governmental organisations such as the United Nations deteriorates, and private powers rise thanks to their ubiquitous presence. The world is united by code, rather than by international agreements and treaties. In such a scenario, the EU will have failed in its attempt to shape the digital economy in a way that fits its own values and traditions. Gradually, EU law is superseded by code, such as technical specifications of large cloud and edge providers, and smart contracts superseding national contract and tort laws. Algorithmic societies gradually replace traditional nation-state structures, and officially

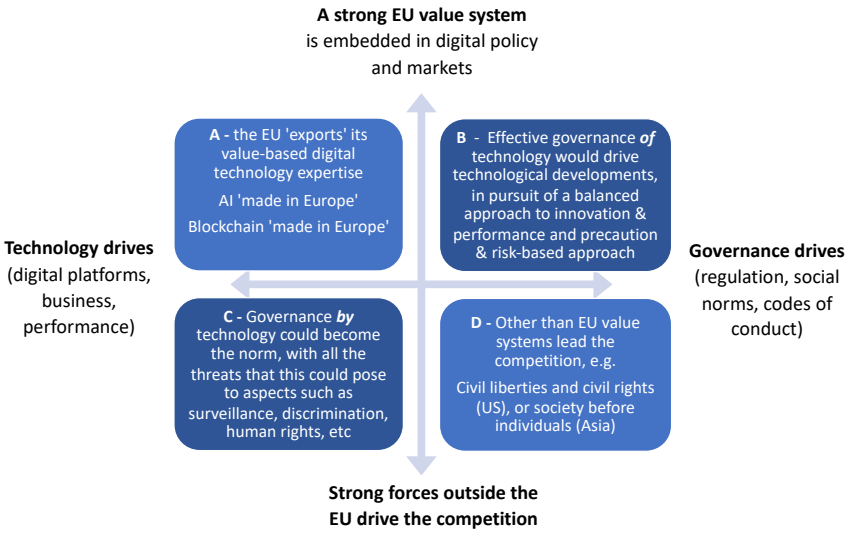
claim to have embedded the pursuit of public goods in their governing algorithms. In this scenario, EU's regulation of AI fails, and private standards (e.g. the tenets of Partnership AI) prevail as global common solutions. Human rights are implemented by code, rather than by jurisdictional remedies. No strong regulation of data quality and no strong competition policy are featured in the (completely digitised) economy. In some countries, surveillance capitalism prevails, whereas in others authoritarian surveillance consolidates. In this tech-enabled world, the boundaries between human and digital blurs, and in the age of extended reality mass manipulation and surveillance becomes by all means possible through the technological architecture. There is very little space for the "Brussels effect" in such as context.

- A strong Europe in a world with strong global governance **(Eutopia)** would entail that the EU's strategy in the green and digital transition (and its successors) has succeeded in restoring Europe's centrality in the global order. Europe's fight for the multilateral order and for global public goods has led the UN and other international organisations to become modernised entities fostering ecological justice, human and non-human rights, and the peaceful cohabitation of the planet. Global institutions and collaboration lead to monitoring global catastrophic risks and, inspired by solidarity, swiftly mitigate the consequences of unforeseen events by taking action in cooperation with the private sector, under efficient orchestration schemes. The EU appears enlarged and stronger, and in a pivotal role especially towards the Global South. In the digital domain, this may also correspond to a situation in which the EU has managed to steer the development of the digital towards EU values, principles, and goals such as trust, fairness, sustainability and resilience. The digital economy evolves in a way that fully leverages the potential of connectivity, AI, DLTs and the Internet of Things to achieve shared prosperity. EU standards on AI regulation and protocols for data spaces gradually impose themselves as global standards, as the EU manages to conquer important spaces in globally governed standardisation bodies. In a scenario like this, no splinternet would occur, and the EU would be able to propose its approach to the digital economy as more balanced than the US "surveillance capitalism", or China's authoritarian surveillance. By actively pursuing technological and data sovereignty for a sufficiently long period of time, Europe could restore its ability to compete at scale in the new frontiers of connectivity (6G-8G) and in the development of AI and IoT solutions for good (beyond the SDGs).
- In the **GAIA** scenario (not to be confused with GAIA-X), global governance has transformed into an effective, stable constellation of actor-network powers operating under a terrestrial systems approach to decision-making and action. These emergent global powers have established strong cooperation based on environmental concerns and balanced with economic and cultural sensitivities to regional conditions. Effective technological regulation and deployment falls under the domain of each global power, and is semi-orchestrated - allowing for regional independence within the guidelines of effective environmental caretaking. While the EU has seen its practical power diminished, its legacy and influence remain within the governance policies set forth in the Gaia Caretakers Framework. While individual nation states have also seen their power diminished, many European national ministries, industrial sectors, and companies remain powerful nodes in the transnational actor-networks. GAIA is effectively a decentralised or a distributed governance scenario. Weak global governance is replaced by a network governance structure, possibly revolving around cities, connected to other nodes in am interoperability framework that extends to semantic and legal interoperability. AI solutions and best practices spread across the different nodes, without a need for a centralised governance structure. Algorithmic governance still preserves the legacy

of EU values and principles, and are optimised thanks to advanced technologies such as quantum computing. In such a scenario, effective technological regulation and deployment falls under the domain of each actor-network, and is semi-orchestrated - allowing for regional independence within the guidelines of effective environmental caretaking. Technological governance is typically conducted by balancing the demands of specific actor-networks with the principles and goals of the Caretakers of Gaia framework. Artificial Intelligence is unevenly deployed across domains, but critical to ecological monitoring and long-term intra-actor-network planning operations. Open Source Software and data standards ensure interoperability and interpretability across Actor Network technologies and lay the ground work for ethical technological development (critical to the GAIA Framework). The EU has ceded ground in R&I activities with the continued rise of more youthful and ambitious populations around the world. AI technologies have been deployed by both state and private actors, though private actors critical role in service provision gives them more power and capability in utilizing incoming data streams. Blockchain and DLTs are central to verifying and incentivizing citizen participation and integrating citizen input into multi-level governance through AI/ML enhanced decision-making.

With these long-term scenarios in mind, a possible shorter-term set of actions for the EU is shown in the figure below.

Figure 9 – Technology, governance and values



4. Concluding remarks: towards an agenda for EU actorness and effectiveness in the digital policy domain

In this report, I have offered a view of the EU's evolving relationship with the features and ongoing development of the digital economy, also based on input received from three other papers that the TRIGGER research team has been able to develop over the first 18 months of the projects' life. The picture that emerges

suggests that the actorness/effectiveness conceptual framework adopted by TRIGGER provides a very clear framework for analysing the positioning of the EU in various policy domains. As a matter of fact, the von der Leyen European Commission seems to be taking action to focus on areas in which it has a greater actorness (e.g. on climate, rather than on rule of law); and in the digital domain, it is strengthening its actorness by building at once a strong regulatory framework, and trying to couple it with a stronger commitment to investment in the full technology stack, flanked by a technological sovereignty narrative. Key, in this endeavour, is the combined weight of two strong personalities like Vice President Vestager, and Commissioner Breton.

This report also showed that the EU faces both short-term and long-term challenges when it comes to strengthening its actorness and effectiveness in the digital domain. Key short-term challenges include completing and modernising the regulatory framework for AI and IoT; define the governance of cloud and data spaces in a way that effectively embeds compliance with EU rules and principles; promote investment through public funding and large government-industry coalitions such as IPCEIs in the domains considered to be most strategic; and develop a strategy at the international level to ensure that EU standards act as reference for the global community. This latter aspect includes the adoption of a proactive stance towards global dialogue in key fields such as AI, the future of work, cybersecurity and 5G, also to avoid a dramatic "splinternet" scenario.

This also amounts to a set of initiatives to address all seven dimensions of actorness:

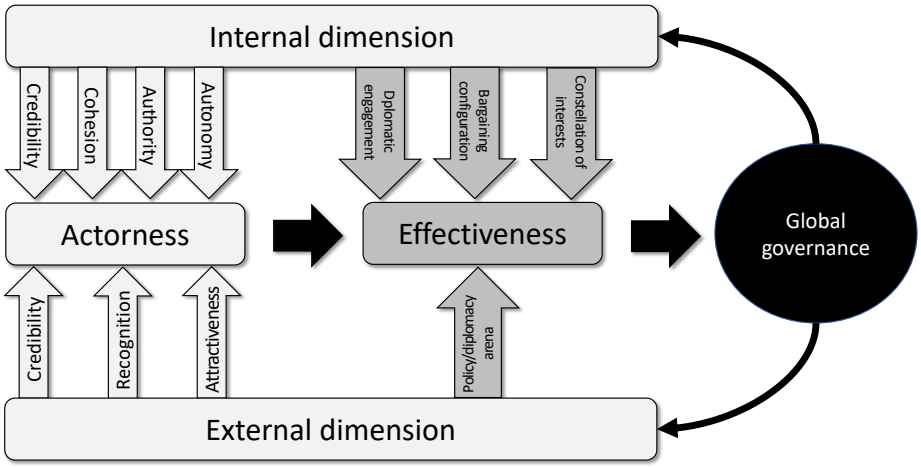
- *Authority*. Further consolidate EU competences in key fields such as competition policy (with an expansion of DG COMP's mandate to include the "new competition tool"); a stronger EU stance in key high-actorness areas such as trade, and adequacy negotiations on data protection; and exclusive competences to orchestrate Member States' actions in the context of AI (Coordinated Plan) and edge/cloud (new IPCEI).
- *Autonomy*. More resources for the twin transition and for AI, compared to the current commitments in the new MFF, which appear to be disappointing at best after the difficult agreement reached between Member States on 20 July 2020. Greater autonomy also means a larger, qualified staff in charge of strategic advice in the digital domain, including in the EEAS; and more resources for intelligence and foresight analysis such as the one offered in this report, in order to guide strategic actions in foreign policy.
- *Cohesion*. The Coordinated Plan on AI and the emergence of a more coherent framework around the notion of "trustworthiness" are first steps towards a much stronger cohesion in EU digital policy. Next steps will rest on the ability of the Commission to orchestrate at a pan-European level the cloud, edge, IoT and data spaces that compose the Single Market 2.0, as described above. Cohesion also means full coherence and consistency between the actions adopted at the EU level in the digital domain, and those undertaken in internal and external action by EU institutions and Member States in all areas of policy that are affected by the digital transformation. In this respect, the twin transition should find a precise and coherent implementation also in the better regulation agenda.

- *Recognition*. The EU should capitalise on the recognition it gained through the GDPR as much as possible, by adding new and more modern items to the list of legal and regulatory frameworks that consolidate its "third approach" to digital policy. The Digital Services Act, the New Competition Tool and the Data Act are a trio that can further nurture Europe's high recognition in this field, making it more long-lasting. At the same time, Europe should step up its research efforts, in order to conquer new areas of recognition also in the field of standardisation and academic research, a field in which European countries have been traditionally strong, but have lately been increasingly outcompeted by their American and Chinese colleagues. At the industrial policy level, the impact of building "European champions" has not been fully and duly researched to date: Europe's recognition could be increased by a policy approach the privileges decentralised architectures, interoperability and the fair distribution of value within given digitised ecosystems, rather than the tardive replication of a model that, initially a formidable engine of growth, has lately shown worrying signs of unsustainability from an economic and social perspective.
- *Attractiveness*. Europe's Single Market should remain open to the rest of the world, but in a way that does not compromise on the vision for the Single Market outlined in Section 2.3 above. The extension of Europe's commercial relationships and data flows would benefit from a more proactive approach, in particular to transatlantic relations, but also, more generally, to digital diplomacy. In this respect, Europe's increasing complementarity with the United States and affinity with Canada and Japan on key policy dossiers such as AI and data policy, and a "negative differentiation" situation in data protection, with countries like India and Brazil taking strong inspiration from the GDPR, will be a strong asset in the future. At the same time, becoming a leader in digital technology for sustainable development would transform the EU into an extremely attractive partner for developing countries that already are attracted towards the *acquis communautaire*, such as many Latin American and African countries that share, at least partly, the same legal tradition of continental Europe; and in addition face the key problem of having to ensure that the deployment of technology leads to effective shared prosperity, rather than the replication of polarised, unequal or undemocratic business models.
- *Opportunity/necessity to act*. The post-COVID-19 transition adds urgency to an already existing trend towards a unique alignment of opportunities. The growing controversies surrounding the Silicon Valley model, described as surveillance capitalism, must now be seen against the lens of the dramatic economic consequences of the pandemic, which showed an extremely fragile labour market, as well as a lack of adequate resilience in the American economy. The excesses of the Chinese social credit scoring system have become even more visible during the COVID-19 emergency, with social control reaching unprecedented levels. The escalation of US-China rivalry leads at once to a deviation of useful resources towards military and defence applications, which hardly address the outstanding societal challenges the world is facing, even more after COIVD; and to the opening of a vacuum that Europe can try to fill by establishing itself as a third power. That said, the transition from the cloud to the edge/IoT environment constitutes a once-in-a-generation chance for Europe, calling for urgent action before the window of opportunity closes. Finally, even if one ignored the positive opportunities offered by the current evolution of global governance, Europe needs to act also to avoid being squeezed between its two larger competitors: very little will remain of the European model unless EU principles, values and laws are converted swiftly into bargaining chips, and lines of code.

- *Credibility and trust*. The EU has the responsibility to restore trust in technology, as a way to restore trust in its model. A credible EU in this respect is also able to promote both an ecosystem of excellence (i.e. resilience and sustainability), and an ecosystem of trust (i.e. rules and initiatives aimed at promoting the responsible and sustainable development of digital technologies throughout the territory of the Union). Already a credible and respected player, the EU also needs to convince its Member States to embark in the twin transition: ironically, perhaps the most difficult front on the side of credibility and trust is the internal one, especially given that the Member States seem to be increasingly forming well-defined clusters (i.e. the "frugal four", the Visegrád countries, the Franco-German axis, and the "South").

The determination and commitment of EU institutions to work on actorness appears as a necessary but still not sufficient condition for the EU to become a more effective player in this space. Effectiveness, defined as 'goal attainment' depends on several factors such as the international context, which looks into the power and international constellation of interests; the process of international negotiations; internal EU politics and negotiation strategies and diplomacy. Moreover, following Peters (2016), a key role will be played by the quality of EU digital policy, in particular its success, leading to the consideration of factors such as output effectiveness, outcome effectiveness, and impact effectiveness. Figure 10 below describes the TRIGGER conceptual framework for actorness and effectiveness, showing that the latter affects directly, via feedback loops, the authority, credibility, recognition and attractiveness of the actor at hand. Output effectiveness can affect directly the opportunity space, as the concrete output of the policy actions emerge as a result of the interaction with other actors' strategies

Figure 10 – Actorness and effectiveness in TRIGGER



Source: Jacob et al. (2019)

As suggested by this approach, even with the most effective effort in place, the EU's level of goal attainment will still largely depend on the strategic choices of other superpowers such as the US and China. A dense web of international cooperation, a clear set of values and principles to offer as a non-negotiable bundle in any international negotiation, a vocation to help the development of third countries on their territory and a clear

stance for global public goods will be needed to ensure that Europe can sustain an otherwise uphill battle in its quest for the spotlight in global governance.

INSTITUTION EURASIAN INSTITUTE
OF INTERNATIONAL RELATIONS

trigger

Trends In Global Governance and Europe's Role

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement nº 822735. This document reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.