triggerX

Trends In Global Governance and Europe's Role

D4.4 Cross-cutting themes from tasks 1, 2 and 3: principles and guidelines for an overarching governance framework

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:	D4.4 Cross-cutting themes from tasks 1, 2 and 3: principles and guidelines for an overarching governance framework
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

Cross-cutting themes from tasks 1, 2 and 3: principles and guidelines for an overarching governance framework

TRIGGER Working paper – deliverable D4.4

Andrea Renda, 31 July 2020

Over the past three decades, the emergence of the digital economy has created both opportunities and challenges for the European Union, affecting its ability to shape both global and internal governance. On the one hand, EU policymakers have often presented Europe as a laggard in terms of digital innovation, dwarfed by the gigantic investments and the ubiquitous footprint of tech giants from the United States and China. On the other hand, the EU has gradually risen to the challenge by becoming an increasingly recognised standard-setter in this domain, in a way that echoes consolidated literature on the EU's normative power. Thanks to its emphasis on the protection of fundamental rights and the pursuit of sustainable development, Europe is now trying to position itself as a "third option", somewhere between the US "surveillance capitalism" and the Chinese "authoritarian surveillance". This aspirational goal is reflected in many policy initiatives of the European Commission, from the ongoing emphasis on open standards and interoperability to the EU policy approach to emerging technologies such as Artificial Intelligence (AI) and Distributed Ledger Technologies (DLTs), as well as recent priorities set in the "Shaping Europe's Digital Future" communication released on February 19, which included also a White Paper on AI and a Communication on a EU Strategy for Data.

These trends, mapped in three thematic papers completed in the context of the TRIGGER (hereinafter, the "TRIGGER papers"), show an increasingly assertive Europe in an increasingly turbulent global governance context. The rise of the "digital cold war" between the United States and China, with escalating investment in digital technologies such as AI and the Internet of Things, leaves Europe with the imperative to seek enhanced technological sovereignty and reduce its dependence on foreign superpowers, especially for critical infrastructure. The COVID-19 pandemic, accompanied by a massive migration to the online world and an unprecedented spread of disinformation, has made connectivity and more generally strategic autonomy an even higher priority on the table of EU decisionmakers. Ursula von der Leyen, President of the European Commission since December 2019, has responded by reiterating the importance of the "twin transition" (green and digital) as the overarching growth strategy of the European Union: this set of priorities was confirmed in the recent agreement on the Multiannual Financial Framework 2021-2027, which for the first time gave the possibility for the European Commission to leverage own resources outside of the contribution of Member States, by borrowing money directly from financial markets.

This paper takes stock of current developments in digital technology, with a view to discussing future avenues for EU and global governance. Accordingly, Section 1 below summarises the main foundations of the digital economy, the main trends observed in the first three decades of the Internet and the challenges they pose for regulators, particularly EU ones. Section 2 summarises the additional insights emerging from the TRIGGER papers, in particular for what concerns technologies such as machine learning and DLTs; and the EU's approach towards openness and interoperability, both in standardisation and in software architectures and solutions. The same section also discuss emerging tensions and the evolution towards a new approach to the Single Market. Section 3 discusses current EU actorness and effectiveness in the digital domain and analyses the possible evolution of the EU and the global governance of digital technologies.

1. Anatomy of the digital transformation

The digital economy gradually brought a paradigm shift in the way economic transactions and social relationships are organised, causing significant problems for policymakers, who traditionally rely on rules and standards built for the "brick and mortar" economy. From the protection of intellectual property rights to the enforcement of competition rules, the formulation of industrial policy and the treatment of the collaborative economy, lawmakers and regulators have been faced with unprecedented challenges in trying to promote and encourage innovation, at the same time creating a level-playing field between legacy operators and new players. Most notably, regulators also face a "pacing problem" (Marchant 2011): given the speed of innovation in the digital economy, regulatory issues often look different at the end of the policy cycle, compared to what they looked like when regulators decided to act.

Against this background, it is important to recall that digital technologies are difficult to encompass and understand for regulators, since they are neither good nor bad: they are "enabling" technologies, which can be used to virtuous as much as vicious purposes and can help regulation as much as they can disrupt it. To be sure, digital technologies are potentially very powerful means to promote wider consumer choice and enhanced competition, stronger competition and greater subjective well-being, but these highly commendable outcomes are far from guaranteed: hence, regulation is called to play a role in mitigating the risks of digital technologies, at the same time maximizing their benefits. Such role implies strong regulatory oversight, careful planning and assessment of alternative policy options in the ex ante phase of the regulatory governance cycle, careful monitoring and regulatory vigilance (Coglianese 2019), as well as the recurrent consultation of stakeholders, who are often more informed than regulators, and reliance on comprehensive ex post evaluations. At the same time, digital technologies have induced regulators to rely more extensively on adaptive, flexible and experimental regulatory schemes, including regulatory sandboxes, as well as various forms of self- and co-regulation.

More in detail, some features of the digital economy have critically affected legacy regulatory schemes based on traditional market structures in which marginal costs are significant, physical investment in assets is needed in order to guarantee adequate stability in service provision, competing products appear reasonably similar in the eye of the end user and both sellers and buyers operate in the same jurisdiction. A recent contribution from the OECD (2018) highlights that market players in the digital economy can achieve "scale without mass" and operate across borders without being established in any significant way on the territory of the markets they serve; and the fact that they increasingly rely on intangible assets and on business models based on network effects, user data and (in most cases) user participation. These features are powered by defining characteristics of digital markets, including direct and indirect network externalities, unprecedented economies of scale, switching costs and lock-in effects, and product complementarity. Such characteristics are increasingly accompanied by other, relevant factors that affect the activity of sectoral regulators: the increased "virtualisation" of functions in digitized value chains; the ongoing "servitisation" of the economy (sometimes referred to as "uberization"); the ongoing "platformisation" of the digital economy; the emergence of distributed and decentralized architectures that challenge the traditional dynamics and structure of markets; and the growing role of AI throughout the technology stack (Renda 2019).

The features of the evolving digital economy have already posed challenges to regulators in several policy domains. For example, the combination of the "scale without mass", "end-to-end" and neutrality features of the Internet ecosystem gave rise to a fundamentally new way to distribute content on the Internet already in the early 2000s, leading regulators and courts to realize that the existing copyright framework was largely inadequate to contain massive infringing behaviours; the ongoing platformisation of the Internet, fostered by network externalities and the enormous growth in online content availability led to a growing concentration of power in the hands of a few online platforms, with consequent calls for antitrust scrutiny and new forms of regulation; the provision of goods and assets "as a service" raises potential challenges in terms of liability and territoriality, remuneration of labour and definition of policies for Artificial Intelligence; and finally, the enforcement of legal rules is increasingly contractualised and privatised.

1.1. The ICT ecosystem: foundational elements

The foundational, differentiating features of the digital economy are summarized below.

- *Computing power and Moore's law*. The digital economy is largely based on the increase in computing power, which has for decades been governed by Moore's law. According to this law, formulated in 1975 by Gordon Moore, the number of transistors – the fundamental building blocks of the microprocessor and the digital age – incorporated on a computer chip will double every two years, resulting in increased computing power and devices that are faster, smaller and lower cost. In other words, computing dramatically increases in power, and decreases in relative cost, at an exponential pace. While this feature of computing power initially concerned mostly hardware devices, with the advent of the Internet age and cloud computing exponential improvements are increasingly observed also in terms of broadband connectivity and digital storage.

- *Modularity (product complementarity)*. The development of increasingly complex products has led engineers to adopt a modular architecture since the early days of microcomputers. As already mentioned, the personal computer launched by IBM in 1981 became an enormous success in terms of market uptake in particular due to its modular architecture, which led many industry players to converge on a single *de facto* industry standard (Bakos and Brynjolfsson 1999; Shapiro and Varian 1998). The Internet adopted a similar modular structure, with multiple tiers of Internet Service Providers, hardware component that run the network and allow for data processing, storage and communication, a "logical layer" that determines traffic flows and exchange protocols, operating systems that govern the interaction between users, devices, the network and information flows; applications that allow end users to carry out a growing number of activities; content generated by users or by third parties; and the users themselves.

- *End-to-end architecture and neutrality*. Being based on the telecommunications network and on open protocols, the Internet-based economy most often features an end-to-end architecture. An end-to end architecture implies the possibility, for every end user, to engage in communication and exchange information with every other end user. The early Internet coupled this feature with the so-called "neutrality" principle, according to which no central intelligence would be able to filter or manage traffic flowing between end users, thus making the Internet a "dumb" network, in which intelligence would be distributed only at the edges (i.e. end users). The Internet Protocol governs the way in which content is protected from inspection through a feature called "protocol layering" (see Yoo, 2013). However, as the Internet started to diffuse and permeate several other economic sectors, its neutrality features started to be increasingly questioned: the impossibility to inspect traffic on the network and to differentiate between applications that require real-time delivery and the ones that are more tolerant to delays have started to constrain technological development in a number of fields, from content and video streaming to online payments. Today, the end-to-end architecture appears as a crucial feature of most business models in the digital economy, whereas neutrality has been largely abandoned in favour of more complex and potentially more effective architectural design (Clarke and Claffy 2015).

Box 1: Is Moore's law coming to an end?

There is a lively ongoing debate on the possibility that Moore's law will come to a halt, and that accordingly, technological progress will slow down in information technology. However, this appears to be a very narrow perspective on the ongoing development of IT hardware, for several reasons.

First, simply counting the number of transistors in integrated circuits does not capture the architecture and performance of modern computer processors (e.g. GPU, TPU). Rather than focusing strictly on increasing transistor counts and clock speeds, companies now focus on performance, including power efficiency and component integration. The explosion of specialized processors for handling AI and deep learning workloads is partly a reaction to the fact that CPUs do not scale the way they used to.

Second, the current trend in designing processors is to move from general-purpose machines to the tailoring of machines to specific applications, such as graphics and machine learning. Today, CPUs co-exist with GPUs (which improve performance by a factor of 10 over CPUs) and TPUs (which improve by a factor of 10 over GPUs). CPUs perform the main tasks, GPUs do the graphics, TPUs the AI.

Third, and relatedly, the emerging trend in IT is 'parallel computing', which achieves exponential growth in throughput by using a multitude of processors at the same time, regardless of the fact that the growth of transistors in integrated circuits is slowing down.

The race for improving computational capacity and performance is thus much more vibrant than a simple, one-dimensional observation such as Moore's law can describe. The state of the art today implies the application of distributed deep learning (DDL) algorithms to GPUs for high-speed data movement, to empower machines to ultimately understand images and sound. The DDL algorithms 'train' on visual and audio data, and more GPUs will mean faster learning. DDL has progressed at a rate of about 2.5 times per year since 2009, when GPUs went from video game graphics accelerators to deep learning model trainers. Next steps will entail the growing use of GPUs, the use of early quantum computers coupled with low precision and analogue devices (as they can tolerate imprecise data and information) to lower power and improve performance (so-called neuromorphic computing); and ultimately, after 2025, the fully-fledged quantum computing era. Current developments in quantum computing appear to be squarely in line with Moore's law. Another likely development that may shake the world of computing is the rise of biological computers (or biocomputers), which typically perform operations using complex molecules such as DNA, could perform huge numbers of parallel calculations at once, and have been in development for decades.

The bottom line is: even if Moore's law slows down, computing will continue to progress at very fast pace, thanks to parallel computing, neural network structures, and quantum technologies. As Moore's law becomes obsolete, technologies will find new ways to support the growth of applications, content, and other hardware.

- *Digital information goods ("scale without mass").* The ICT ecosystem is essentially based on digital technology, and as such features many of the characteristics that information displays from an economic perspective. Since Kenneth Arrow's characterization of information and the advancement of theories of common pool resources and the so-called "information semicommons" (Heverly 2003), the understanding of the peculiar economics of information has evolved significantly in social sciences. The fact that goods and services offered on the Internet are made of 0s and 1s (i.e. digitized in binary language) bears significant consequences for the economics of the sector. These include: (i) *endless replicability and non-rivalry in consumption*: information goods can be replicated with no significant loss in quality, and can be accessed by different users from multiple locations at the same time, thus enabling sharing: (ii) *near-zero or zero marginal costs*: replicating the information embedded in an information good normally costs nothing (today, in most cases there is no need for a physical device to contain the information good, as in the case of downloaded content and software); (iii) *plasticity and granularity*: digital information (and related goods) can be decomposed, rebuilt and repackaged *ad libitum*, thus leading to endless possibilities for versioning, sampling, re-use, including through user-generated content, text and data mining and many other activities.

These foundational characteristics have determined the emergence of some key features that are typically attributed to the digital economy by scholars and industry analysts. For example, Goldfarb and Tucker (2017) argue that the digital economy typically displays five categories of shifts in costs: (i) lower search costs; (ii) lower replication costs; (iii) lower transportation costs; (iv) lower tracking costs; and (v) lower verification costs. In terms of innovation, the impacts to be expected are the following:

First, *R&D intensity and innovation rates tend to be greater than in other sectors*. This depends on a number of factors, including the acceleration in computing power (Moore's law); the possibilities for diffusion guaranteed by the common architecture (Metcalfe's Law); and the possibilities for participation secured by the choice of open protocols (i.e. anyone can in principle develop a software or hardware that is compatible with existing Internet protocols).

Second, *innovation was initially largely incremental, due to modular architectural design* that followed "big bang" inventions such as the computer chip and the Internet protocol: this feature is however not as evident today due to the platformisation of the Internet; however a number of economic sectors are being permeated by new and disruptive business models and technological breakthroughs, especially in the field of High Performance Computing, the IoT and Artificial Intelligence.

Third, *product life-cycles become increasingly shorter due to the acceleration of technological change*: several companies in the ICT ecosystem (and even more, the ones active at the higher layers, such as operating systems, other middleware, and applications) reportedly work on at least three successive generations of products (the current one, the next one, and the one after that).

Fourth, *the end-to-end architecture of the Internet and the digital nature of information goods have led to the emergence of network effects and large economies of scale* in the ICT ecosystem: this, in turn, has led to the emergence of multi-sided platforms that are gradually changing the architecture of the network.

All these aspects bear consequences in terms of innovation performance/dynamics, industry performance, competition, overall societal welfare, and of course regulation and international regulatory cooperation.

1.2. The evolving ICT ecosystem: main trends

In this section four main trends that are affecting the ICT ecosystem are described: the "platformisation" of the ecosystem, which implies the emergence of large online digital intermediaries; the increased virtualization of various parts of the ecosystem; the virtualization of functions in the Internet architecture and the emergence of cloud computing; the rise of open and collaborative business models, often involving (at the higher layers) open IP strategies such as open source software and open patent portfolios; the growing prominence of big data and data-driven innovation; the rise of artificial intelligence as a family of digital technologies that pervades all layers of the technology stack; and the increasing attractiveness of distributed and decentralized architectures such as Distributed Ledger Technologies.

1.2.1. The end of Moore's Law?

In hardware, current trends include virtualisation of functions, massive cost reductions, and the transition from central processing units (CPUs) to more efficient and powerful graphics processing units (GPUs) and ultimately tensor processing units (TPUs), designed as AI accelerators. However, the real discontinuity will arrive in a few years, with quantum computing taking the stage and becoming commercially viable. This means an impressive acceleration in the ability of computers to solve complex problems, from logistical and optimisation problems to weather and climate modelling, personalised medicine, space exploration, real time language translation and, most generally, encryption.

There is a lively ongoing debate on the possibility that Moore's law will come to a halt, and that accordingly, technological progress will slow down in information technology. However, this appears to be a very narrow perspective on the ongoing development of IT hardware, for several reasons:

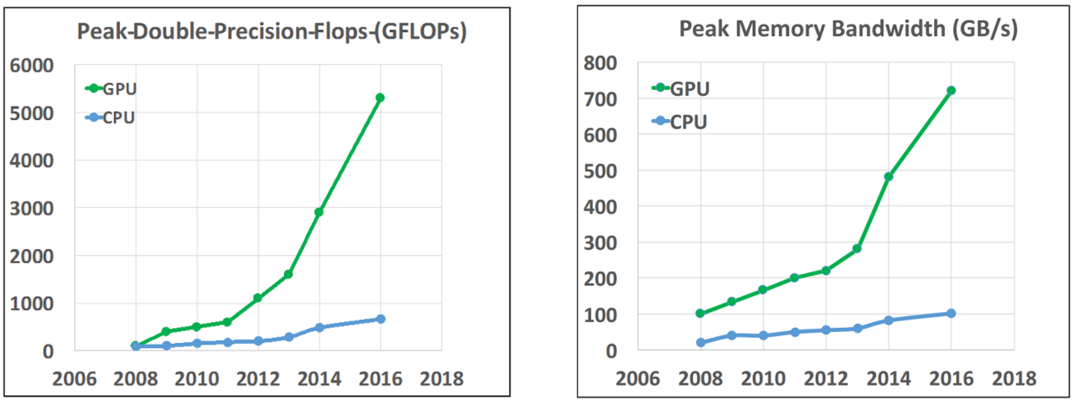
- First, simply counting the number of transistors in integrated circuits does not capture the architecture and performance of modern computer processors (e.g. GPU, TPU). Rather than focusing strictly on increasing transistor counts and clock speeds, companies now focus on performance, including power efficiency and component integration. The explosion of specialised processors for handling AI and deep learning workloads is partly a reaction to the fact that CPUs do not scale the way they used to.

- Second, the current trend in designing processors is to move from general-purpose machines to the tailoring of machines to specific applications, such as graphics and machine learning. Today, CPUs co-exist with GPUs (which improve performance by a factor of 10 over CPUs) and TPUs (which improve by a factor of 10 over GPUs). CPUs perform the main tasks, GPUs do the graphics, TPUs the AI.

- Third, and relatedly, the emerging trend in IT is 'parallel computing', which achieves exponential growth in throughput by using a multitude of processors at the same time, regardless of the fact that the growth of transistors in integrated circuits is slowing down.

Looking at emerging new processors, the transition from CPU to GPU also implies a transition from incumbent chip manufacturers Intel and Advanced RISC Machine (ARM) towards players like Nvidia. And the rise of TPUs sees Google in the lead. While CPU performance improvements have been slow over the past few years, GPUs are progressing faster than Moore's law. GPUs are also more appropriate for parallel computing; they are eventually expected to replace CPUs entirely. Currently, CPUs and GPUs interact and co-exist, and some available processors are hybrid solutions (e.g. Intel's *Knights Landing*). It is eventually possible that the AI and deep learning processors deployed in data centres will be different from those deployed at the edge, in smartphones, wearables, PCs. When compared on a chip-to-chip basis against CPUs, GPUs have significantly better capability on both speed of calculation (FLOPS) and speed of data movement (bandwidth) (GB/s) (Figure 1).

Figure 1. Improvement in processing capacity



Source: HPC 2016.

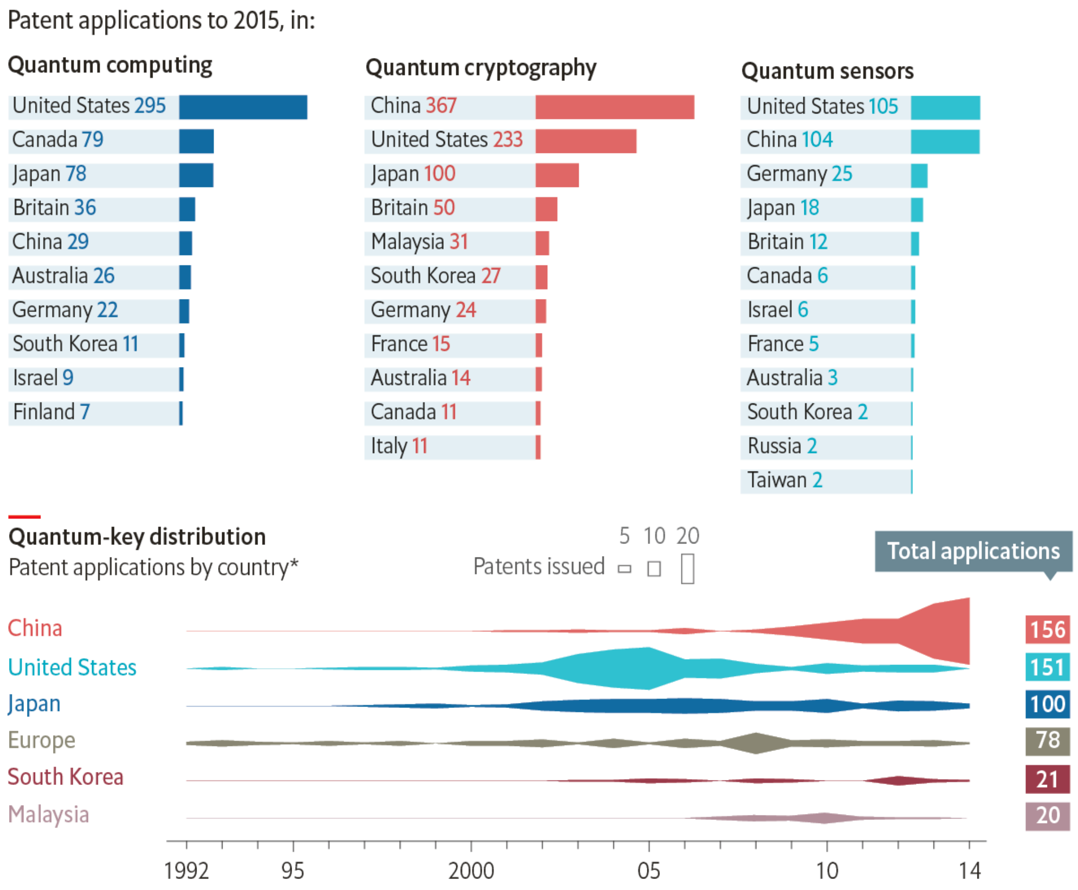
The race for improving computational capacity and performance is thus much more vibrant than a simple, one-dimensional observation such as Moore's law can describe. Intel, for example, after seeing its CPU threatened by GPUs, started to compete head-to-head with NVIDIA and AMD with x86-capable 'manycore' chips. Google, with its TPUs, mostly aims at developing superfast computers for machine learning applications.

The state of the art today implies the application of distributed deep learning (DDL) algorithms to GPUs for high-speed data movement, to empower machines to ultimately understand images and sound. The DDL algorithms 'train' on visual and audio data, and more GPUs should mean faster learning. DDL has progressed at a rate of about 2.5 times per year since 2009, when GPUs went from video game graphics accelerators to deep learning model trainers. Next steps, according to tech companies like IBM, will entail the growing use of GPUs, the use of early quantum computers coupled with low precision and analogue devices (as they can tolerate imprecise data and information) to lower power and improve performance (so-called neuromorphic computing); and ultimately, after 2025, the fully-fledged quantum computing era.

There is still lots of uncertainty regarding the foreseen evolution of quantum computing. The Canadian company D-Wave Systems has already progressed from a computer with 128 qubits to an upcoming machine with 1,000. IBM has made a 20 qubits computer commercially available. A 50-qubit quantum computer already manages 300 TB of information, and potentially reaches 'quantum supremacy', i.e. a quantum device able to handle such a number of registers that no single classical device on Earth can keep up with it. A quantum computer with 50 qubits would be smaller, more powerful and more energy-friendly than the best existing classical computer on Earth. At 100 qubits, a quantum computer would surpass by far the number of options that can be stored in all the classical computers on Earth combined. Companies like D-Wave expect to be able to quadruple the number of qubits every two years, ultimately reaching a million qubits in 2035. However, the race is hectic, with incumbent players like Microsoft, Google, IBM and newcomers like D-Wave and Rigetti all pushing to be the first to develop a stable and sufficiently powerful quantum computer.

Future applications of quantum computing are widespread, ranging from the solution to complex cryptographic problems to the simulation of drug response to greater understanding of disease development through improved computational models, improved transportation logistics across the world, improved financial modelling to avoid economic downturns, and more. Not surprisingly, countries are racing to develop quantum computers, with the US and China competing neck and neck. The figure below shows however that recent years have seen Chinese patent applications skyrocket. This race has very important geo-political consequences: it is generally understood that global leadership and supremacy in the future will depend on the control of key IT such as quantum computing. China recently announced that it will create an 11 billion USD, four-million-square-foot national quantum laboratory in the city of Hefei. Russia is investing in quantum computing, spearheaded by the Russian Quantum Center (RQC). In the twenty-first century, supremacy will belong to the nation that controls the future of information technology, which is quantum. As we will see, it would be a mistake to assume that the United States is destined to be in this position. In the topsy-turvy, counterintuitive world of quantum mechanics and quantum computing, decades-long dominance in IT does not automatically translate into dominance in the coming era. However, strategy and commitment of resources, including funding, almost certainly will – and with it, the balance of the future.

Figure 2. Evolution of patent applications by country



Sources: UK Intellectual Property Office; European Commission

*By location of corporate headquarters

Another likely development that may shake the world of computing is the rise of biological computers (or biocomputers), which typically perform operations using complex molecules such as DNA, could perform huge numbers of parallel calculations at once, and have been in development for decades. The EU funded a project (Bio4Comp) in this area with 6.1 million euros, in the belief that biocomputing could overcome the scale limits of quantum computing, as well as other experimental models such as DNA and microfluidics-based computation. Recently, Intel announced Loihi, a neuromorphic chip that can count on a total of 130,000 neurons and 130 million synapses (Reichert, 2017). Loihi is a 60-mm^2 chip fabricated in Intels 14-nm process that advances the state-of-the-art modelling of spiking neural networks in silicon. It integrates a wide range of novel features for the field, such as hierarchical connectivity, dendritic compartments, synaptic delays, and, most importantly, programmable synaptic learning rules. Running a spiking convolutional form of the Locally Competitive Algorithm, Loihi can solve LASSO optimisation problems with over three orders of magnitude superior energy-delay-product compared to conventional solvers running on a CPU iso-process/voltage/area. This provides an unambiguous example of spike-based computation, outperforming all known conventional solutions.

The bottom line is: even if Moore's law slows down, computing will continue to progress at very fast pace, thanks to parallel computing, neural network structures, and quantum technologies. As Moore's law becomes obsolete, technologies will find new ways to support the growth of applications, content, and other hardware.

1.2.2. From the "neutral" to the "platformised" ICT ecosystem

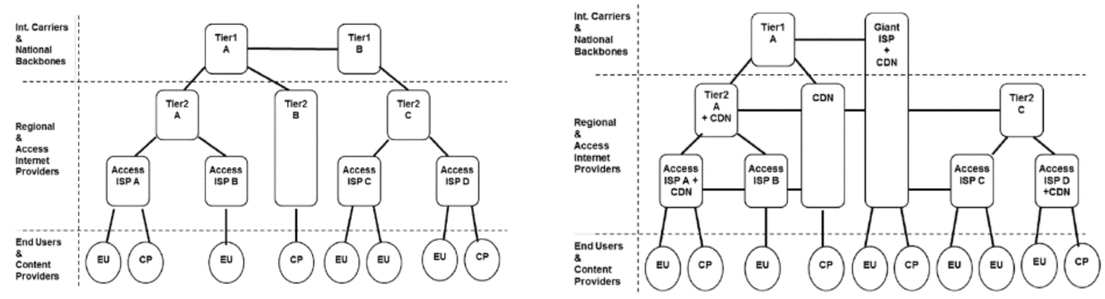
A number of authors have illustrated the ongoing transformation of the digital economy, mostly due to the advent of the Internet as a major form of communication. The explosion of Internet traffic in the 1990s and 2000s, powered by parallel streams of evolving technologies (data storage, broadband communications, 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.

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. Learning effects, direct and indirect network externalities determined the need for the market to "tip" in favour of one standard, rather than preserving a wide array of competing products. Microsoft adopted for its Windows application (later, OS) an architecture that would maximize the potential of indirect network externalities: just as VHS won the standards war with Betamax in the video-recorder era due to a greater number of applications, Windows won over its competitors by focusing on the number of applications that would be compatible with its standards, be they developed in-house or by third parties. By becoming a platform for third party applications, Windows could exploit self-reinforcing, centripetal forces: the more an OS becomes popular among its end users, the more developers will want to develop applications compatible with that OS; and vice versa, the more apps are available to end users, the more the latter will find switching to another OS unattractive. The age of platforms had officially begun: today, the economics of platforms has become a stand-alone field of research in economics and in other social sciences, encompassing management, strategy, industrial economics, social network analysis and many more (Spulber 2018).

The emergence of the Internet exacerbated this feature. Network effects in broadband communications were increasingly flanked by direct and indirect effects generated by platforms and applications, making the digital ecosystem a peculiar environment, in which leading platforms rise and fall in just a few years; and in which attracting user attention becomes the most important source of competitive advantage. Terms like "economics of attention" or "competition for eyeballs" have become commonplace when describing the strategy followed in the digital ecosystem by companies like Amazon, Google, Microsoft, or Facebook. These companies present themselves as the new protagonists of the "platformised Internet". Today, the digital ecosystem has evolved into a much more diverse environment in which 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.

As observed *i.a.* by Palacin et al. (2013) and by David Clark and KC Claffy (2014, 2015), this transition is now evident if one confronts the original (three-tier) model of the connectivity and logical layer of the internet ecosystem with the emergence of vertically integrated platforms that make extensive use of traffic acceleration techniques, and developed their own semi-walled gardens to improve their customers' experience and capture the bulk of the end users' attention (figure 3 below). For example, a company like Apple uses Content Delivery Networks (CDNs) like the ones provided by Akamai to deliver faster traffic to its FaceTime users; and at the same time hosts more specialized providers such as Netflix, which in turn use traffic acceleration techniques to enable video streaming services to subscribers through a multitude of existing platforms (iOS, Android, public Internet). A company like Spotify can be defined as a two-sided specialized platform (matching users with rights holders), but access to it mostly occurs through existing large platforms (iOS and Android). This phenomenon, often called "platformisation" of the Internet ecosystem, bears far-reaching consequences for both innovation, and innovation policy. In particular, understanding the economics of platforms is essential to understand the direction and pace that innovation might take in various parts (layers) of the Internet ecosystem, as will be discussed in the next section.

Figure 3. Old v. new Internet: platformisation



Source: Palacin et al. (2013)

Source: Palacin et al. (2013)

The emergence of new forms of platforms has been highlighted as a specificity of the Internet ecosystem. For example, in her attempt to build a unifying theory of business and engineering perspectives on platforms, Annabelle Gawer (2014) observes that three main types of industry platforms have emerged over time in various industries, depending on whether the constitutive agents of the platform are: a firm and its sub-units (in internal platforms); or an assembler and its suppliers (in supply-chain platforms); or, a platform leader and its complementors (in industry platforms). That said, all platforms share a common modular architecture organized around a core and a periphery. Moreover, all platforms have technological interfaces (between the "core" and the "periphery") and, depending on whether they are within firms, within supply-chains, or within ecosystems, these interfaces are closed, semi-closed, or open.

Gawer (2013) provides a unified conceptualization of platforms as organizations, as follows. Technological platforms can be usefully seen as evolving organizations or meta-organizations that:

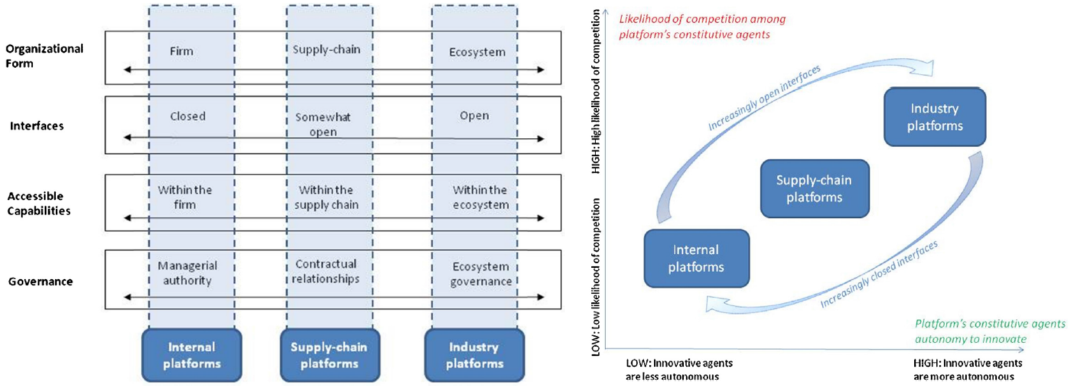
- Federate and coordinate constitutive agents who can innovate and compete;
- Create value by generating and harnessing economies of scope in supply or/and in demand;

- Entail a technological architecture that is modular and composed of a core and a periphery.

Key underpinnings of the study of platforms include the following:

- Especially in the digital economy, given the existence of network effects and the multi-purpose nature of the Internet architecture, platforms can evolve from mere internal coordination mechanisms, into de facto industry-wide platforms.
- In this transition, platform participants can change role and move from complementor producers to platform operators, which raises the issue of intra-platform competition between the pivotal firm and its complementor producers. This is easily illustrated by the example of Microsoft's emergence as a platform leader after having been a complementor producer (producing the OS in IBM's PC); as well as Google's emergence as a platform leader after having started as a complementor producer in the Windows platform. Accordingly, while a large proportion of the platform ecosystem's agents will innovate in ways that are complementary to the platform, a number of them will start innovating in ways that become competitive to the platform.
- Openness typically pays. As platform interfaces become more open, more agents will be attracted into the platform ecosystem, and the platform leader will be able to access a larger set of potentially complementary innovative capabilities (Gawer 2013). In many markets, a tendency towards more open, or semi-open business model has clearly emerged (e.g. Android as a more open business model than iOS), although it is difficult to conceive of a fully open business model, which generates no revenue for any of the players.
- These insights have bridged the economics of platforms and the study of business models and architectures, by showing that ICT platforms are a moving target, and that the dynamics of competition and innovation between them, as well as within them, are likely to vary over time, with platforms likely to move up from purely internal to supply-chain platforms, and finally to industry platforms; and other platforms likely to react to mounting competition by going back from industry to supply-chain platforms. The degree of openness of the relative interfaces is the decisive element in determining the type of platform that is being observed.

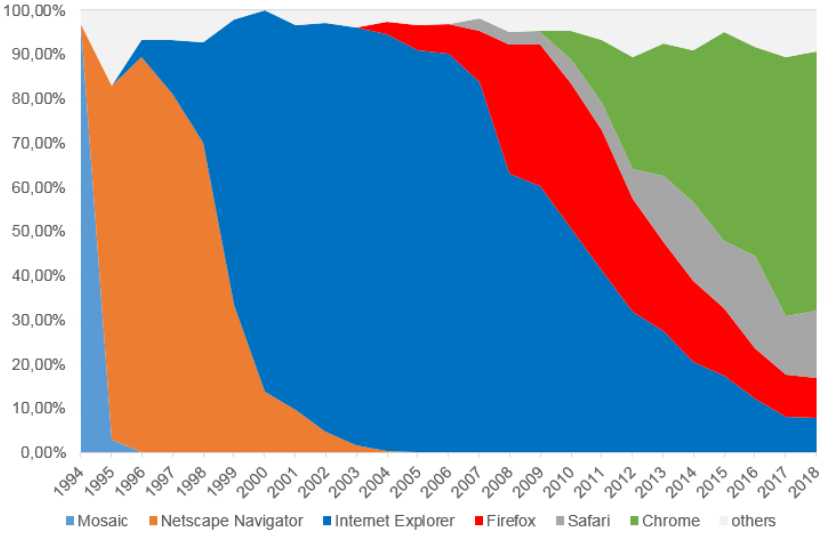
Figure 4. Platforms: taxonomy and life cycles


Organizational Form
Firm
Supply-chain
Ecosystem
Interfaces
Closed
Somewhat open
Open
Accessible Capabilities
Within the firm
Within the supply chain
Within the ecosystem
Governance
Managerial authority
Contractual relationships
Ecosystem governance
Internal platforms
Supply-chain platforms
Industry platforms
Likelihood of competition among platform's constitutive agents
HIGH: High likelihood of competition
LOW: Low likelihood of competition
Increasingly open interfaces
Increasingly closed interfaces
Industry platforms
Supply-chain platforms
Internal platforms
Platform's constitutive agents autonomy to innovate
LOW: Innovative agents are less autonomous
HIGH: Innovative agents are more autonomous

Source: Gawer (2014)

Digital platforms thus rise and fall, changing role and constantly competing to stay relevant. Figure 5 below shows for example the waves of dominant browsers in the period 1994-2018.

Figure 5. Platforms: taxonomy and life cycles



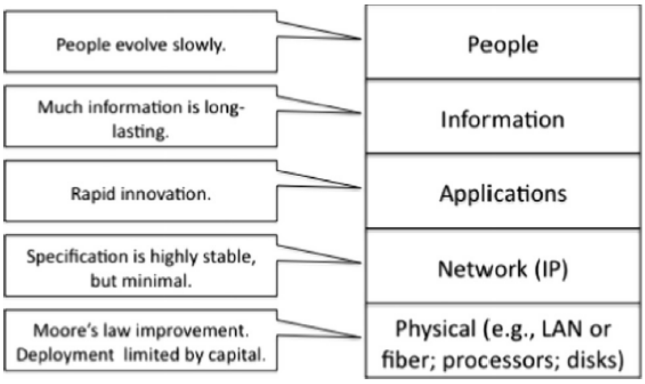
Note: Usage share of internet web browsers with data as aggregated by Wikipedia (see 'Wikipedia' with: W3Counter: 2007 to 2018, TheCounter.com: 2000 to 2007, GVU WWW user survey: 1994 to October 1998/1999). Due to the different sources for the raw data, there are inconsistencies on a minor level, but the general trend is consistent across all available sources. This dataset does not include dedicated browsers for mobile phones. In addition, it does not extend to the current development of voice-based assistants (incl. internet access) such as Amazon's Alexa, Google Assistant and Microsoft's Cortana.

Source: Bött and Milkau (2018)

The platformisation of the internet ecosystem also bears important consequences for the assessment of competition dynamics and in the consideration of possible regulatory actions. First, regulation has to be tailored to the specificities of the different layers that compose the ecosystem: Claffy and Clarke (2014, 2015) observe that in the current Internet ecosystem innovation takes place in different ways across platforms, and across layers, and that the emergence of vertically integrated platforms must be observed also through this specific lens, which proves essential for regulation and innovation policy. They define the ICT ecosystem as a perfect setting for co-evolution and explore the natural rate of change of various components of the ICT ecosystem, where some interdependent actors have a natural tendency to evolve faster than others. In the figure below, the physical (lowest) layer experiences a rate of change gated by labour and sources of capital, neither of which follow a Moore's Law cost function. At the Internet layer (the Internet Protocol, or IP), the durability of the specifications of the core protocols provides a stable foundation for rapid innovation at other layers.

At the application layer, the process of innovation is driven at almost frantic rates that Clarke and Claffy estimate as holding a potential of 10 improvements in underlying technology every 5 years. At the information layer, the creation, storage, search and retrieval of essentially all forms of data – information, content, knowledge – is moving on line. The people level displays a transformative empowerment from the deployment of technology in the hands of humans. But human capabilities in no way grow on a Moore's Law curve. People do not get twice as smart, or twice as capable of processing information, every 18 months. So, users end up drowning in information overload, and call for even more technology to control the flood, which makes us even more dependent on the technology. Again, this leads us back to the economics of attention, and the development of large online platforms.

Figure 6. Layered Internet ecosystem, and pace of evolution


People evolve slowly.
Much information is long-lasting.
Rapid innovation.
Specification is highly stable, but minimal.
Moore's law improvement. Deployment limited by capital.
People
Information
Applications
Network (IP)
Physical (e.g., LAN or fiber; processors; disks)

Source: Clarke and Claffy (2015).

These different paces of technology integration across the ecosystem also influence the stability and agility of firms. Companies that have invested in physical assets like fibre to the home, towers or data centres can sometimes earn a stable place in the ecosystem through that investment, although a bad technology bet can leave them disadvantaged by a stranded investment. Firms with extensive physical infrastructure investments also cannot easily move, and typically remain domestic except by merger and acquisition of firms in other countries. In contrast, firms at higher layers are more likely based on an idea (like Facebook) than on heavy capital investment. The commercial ecosystem experiences constant pressure from application innovators to seek new capabilities from the physical layer (e.g., more capacity to the home), while the investment in those capabilities must be made by a different set of firms. According to Clarke and Claffy (2015), “this tension is a classic example of co-dependency and co-evolution within the industrial part of the ecosystem, where applications are limited in their ability to evolve by the rate at which the physical layer can evolve. Because the application layer depends on the physical layer, the application layer cannot simply out-evolve the physical layer but is gated by it”.

The consequences of the specific features of the ICT ecosystem, as described in the previous sections, are far-reaching to say the least. The interaction of technology, architectural choices and business models that have emerged in the past years determine the emergence of the following peculiarities, which inevitably affect the pace and direction of sound innovation policy in the ICT sector.

- **Infinite possibilities for open and distributed innovation** (in some layers). In the higher layers of the Internet architecture, and in particular from the Internet layer upwards, open and distributed innovation can be organized in a very granular way. Companies can easily organize production through distributed co-creation, or directly by empowering users to promote and produce their innovations. The use of big data and the ease of manipulation and reconfiguration of information goods makes it possible to reach unprecedented, and unmatched, levels of mass customization. Accordingly, nowhere as in the ICT sector open innovation 2.0 flourishes.
- **Regulatory outcomes depend on technology at all layers, as well as by interdependencies and externalities across and within platforms**. What emerges from recent contributions to the

literature is that our understanding of ICT innovation must be enriched to capture the consequences on innovation incentives of interdependencies between components and markets, as well as the potential for value creation that can arise when a set of mutually enhancing business models emerge across the ecosystem. Innovation incentives are thus not only the result of ecosystem interactions outside the platform, but also, importantly and increasingly, of the interactions that are observed inside existing platforms.

- **The end of economies of scale?** This controversial observation is dependent on a number of technology trends, which include: the gradual fall in the cost of IT hardware equipment; the gradual virtualization of hardware components (from cloud-based access to server capabilities to the increasingly widespread availability of traffic acceleration services, and software defined networks); the increasing size and capacity of data storage centres needed to store and process the mass of data being produced on a daily basis; and the possibility, for some players that occupy a pivotal role in the Internet ecosystem, to accumulate and process massive amounts of data.

- **Crowdfunding and other forms of access to credit**. Given the breath-taking pace of innovation at the higher layers of the ICT ecosystem, it is not surprising that some killer applications and innovative products have emerged from successful crowdfunding campaigns, even if the potential of crowdfunding seems to be still uncertain in many fields, and existing platforms in Europe seem to be still mostly a new form of collecting money from family and friends, which seems to occur in as many as 73% of the cases (Gabison 2015). Outside the EU, and in particular in the United States, crowdfunding has already shown that it can provide a market for innovators, especially when large platforms use it or rely on it to add new features to their portfolio of services and applications. For instance, crowdfunding has led to the success of wearables such as the Pebble Watch[1], gaming solutions such as Ouya[2], and Oculus Rift[3], or Robots like Jibo[4]; connected-home systems such as Canary[5], and many more. The same applies to drones, connected-health solutions, and seemingly random gadgets such as the coolest cooler—and they've all been given life from crowdfunding. Over the past few years, the rise of cryptocurrencies and distributed ledger technologies has also led to the emergence of another, increasingly prominent form of crowdfunding of new ventures, which takes the form of an **initial coin offering (ICO)**. In an ICO, a quantity of cryptocurrency is sold in the form of "tokens" to speculators or investors, in exchange for legal tender or other cryptocurrencies such as Bitcoin or Ethereum. The tokens sold are promoted as future functional units of currency if or when the ICO's funding goal is met and the project launches. Banned in some jurisdictions for their ability to. Side-step all intermediaries, ICOs are not seeing a wave of regulation around the world, which aims to preserve their benefits, at the same time reducing the risk of speculation and frustration of investors' expectations.

- **Skills as a main constraining factor?** As discussed above, the human factor appears to be the slowest layer in the ICT ecosystem, as well as an increasingly scarce resource (Grundke, 2018). The European Commission has long denounced the emerging skills mismatch in Europe, looking at the slower pace of skills update compared to technology update: *"skills development does not come about as fast as technological development, which is why we are faced with a paradoxical situation: although millions of Europeans are currently without a job companies have a hard time finding*

[1] https://getpebble.com/

[2] http://www.ouya.tv/

[3] www.oculus.com/en-us

[4] http://www.jibo.com/

[5] http://www.canary.is/

skilled digital technology experts. As a result, there could be up to 825,000 unfilled vacancies for ICT … professionals by 2020". A recent study commissioned by the European Economic and Social Committee estimated that the European economy loses over 2% of productivity per year due to a mismatch of skills, according to a recent study commissioned by the European Economic and Social Committee. This translates into a loss of €0.80 for each hour of work[6]. Accenture (2018) recently estimated that if G20 countries fail to adapt to meet the needs of the new technological era, they could be in line to miss out on as much as $1.5 trillion in GDP growth over the next 10 years.

- **User attention as main entry barrier?** While the political debate on the evolution of the digital economy has been largely dominated by the idea that non-neutral Internet models and the alleged market power of large online platforms (so-called "GAFTAM", i.e. Google, Amazon, Facebook, Twitter, Apple, Microsoft) constitute major barriers to entry for new players (the so-called "new Google" argument, see Renda 2011), reality seems to tell a slightly different story. The ongoing platformisation of the Internet and the rise of so-called "Superstar firms" (Autor et al. 2017) has been accompanied by a concentration of the market at the platform layers, but at the same time seems to be largely reducing barriers to entry at the application and service layers. For example, competition between *i.a.* Google, Microsoft and Amazon for leadership in cloud services is leading these companies to offer zero-price, high quality solutions for app providers in need of key services such as traffic acceleration, data storage, server and other hardware access and usage, big data analytics, and much more (Palacin et al. 2013). And indeed, it seems that in big data applications barriers to entry are not significant, even if it would be reasonable to infer that the availability of a large amount of data could represent a source of competitive advantage for large platform operators[7]. As a result, the real barrier to entry that exists in the Internet ecosystem is user attention, which in turn represents a key resource for companies that adopt advertising-based business models.

- **IPRs: friend or foe for entrepreneurs in ICT?** The peculiarities of the ICT ecosystem, particularly at the higher layers, also bear consequences for government policies such as IPR policy. Many companies in the application and content layers of the digital economy prefer to rely on trade secret rather than on patents or copyright and consider intellectual property rights in general as an obstacle to their innovation efforts, rather than a viable incentive scheme. This is due to a number of factors, which include the following:

  - *The nature of information as often rivalrous, but non-excludable.* (formalized in the literature as Arrow's paradox of information[8]). The fact that ICT innovation consists mostly of information goods, which are easy to replicate and sometimes also relatively easy to reverse-engineer, determines a lack of incentives to use instruments such as patent law, which require the disclosure of the underlying idea.

  - *The "free" nature of many innovative services.* The platformised internet is the locus of free ad-based business models, which *per se* imply that the inventor does not rely on the sale of the product as a source of revenues. This, in turn, makes patent protection less attractive, as related royalties would not be expected by innovators in this field.

[6] https://www.eesc.europa.eu/en/our-work/publications-other-work/publications/skills-mismatches-impediment-competitiveness-eu-businesses.

[7] http://www.project-disco.org/competition/040215-big-data-entry-barrier-tinder-can-tell-us/

[8] Arrow, Kenneth J. (1962), "Economic Welfare and the Allocation of Resources for Invention," in Richard R. Nelson (ed.), The Rate and Direction of Inventive Activity, 609-625.

- *The gatekeeping, self-regulatory role of large platforms*, which ensure through self-regulation and their self-sustaining business model that emerging successful applications are not paralleled by free-riding emulators on the same app store. In this respect, platforms can represent more authoritative gatekeepers than legislators themselves.
- *Problems of strategic behaviour and uneven bargaining power*. These include patent hold-up, royalty stacking, Patent thickets, patent assertion entities, non-practising entities, etc. These practices create inefficient incentives and market outcomes, and further exacerbate the problem of uncertainty.
- *Legal uncertainty and obsolescence.* IPRs are effective means of rewarding innovation to the extent that they mirror the underlying dynamics of innovation. However, there are reasons to believe that current IPR legislation in many OECD countries is hardly in line with the evolving dynamics of the ICT ecosystem.

1.2.3. Virtualisation and the cloud

A second, important trend that is evident in the evolution of the digital economy is the ongoing virtualization of a growing number of functions, again made possible by technological evolution and underlying standardization. With this standardization come significant cost reductions, shifting of market power and user attention, and the disruption of existing business models. Perhaps the most evident trends in this respect are cloud computing and software-defined networking.

With cloud computing, technology has 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" has led personal devices become increasingly light, while users were able to lease software located in the cloud, as well as access their files that are stored somewhere in cyberspace, and managed by a cloud provider: put more simply, a limitless "office LAN" where the main server was not located downstairs, but potentially on the other side of the globe[9]. An industry report defined "cloud implementation" as "an elastic execution environment involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality (of service)"[10].

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 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

[9] 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"

[10] The most widely used definition of cloud is that provided by the US National Institute for Standards and Technology (NIST) in 2009: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

application as a service (AaaS) or software as a service (SaaS) modes[11]. 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.

Already in the 1990s, cyberlaw scholars started to understand that the Internet would have led to the emergence of an "age of access", in which products and services will be dematerialized to an extent that would make ownership and property rights less important, and access rights gradually more dominant[12]. 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.

1.2.4. Openness and collaboration

Another trend that has characterized the evolution of the ICT ecosystem, especially after the advent of the Internet, is openness. The most fast-growing, innovative parts of the ICT ecosystem include the emergence of the collaborative economy and distributed architectures. Here are some important examples to keep in mind.

First, open source software is evolving and growing from the initial models of "copyleft" licensing, based on reciprocity and the voluntary commitment to refrain from claiming the exclusive right to commercially exploit a given invention, towards a variety of models, which include the making available of entire patent portfolios for free exploitation by users and small entrepreneurs. Today, open-source platforms developed through distributed co-creation, such as the "LAMP" stack (for Linux, Apache, MySQL, and PHP/Perl/Python), have become a standard component of the IT infrastructure at many corporations. The exact combination of software included in a LAMP package is not fixed and may vary depending on developers' preferences: for example, PHP may be replaced or supplemented by Perl, Python or Ruby, the OS can be replaced with Microsoft Windows, Mac OS, Solaris, iSeries, or OpenBSD and others; database component also can be replaced, and webservers other than Apache are being used. All this creates a collectively developed environment in which programmers and users co-develop software that powers a large amount of new Web applications.

Second, openness has become an increasingly dominant paradigm also with respect to IPRs. Key examples include, in the public sector, the decision by NASA to make hundreds of patents available for free for developers[13]; and in the private sector, the decision by Google to open up its Android patents[14]; as well as the decision by Tesla's Elon Musk (later followed by other car manufacturers

[11] Renda, A. (2012), Competition, Neutrality and Diversity in the Cloud, Communications & Strategies, No. 85, 1st Quarter 2012, pp. 23-44.

[12] See i.a. Gomulkiewicz, R.W. (1998), "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.

[13] http://www.nasa.gov/press-release/nasa-offers-licenses-of-patented-technologies-to-start-up-companies

[14] http://techcrunch.com/2015/07/23/google-offers-to-sell-patents-to-startups-to-boost-its-wider-cross-licensing-initiative

such as Ford) to open up for free the company's patent portfolio to external developers[15]. This example is being followed by governments: for example, the United States Open Government strategy is increasingly geared towards the diffusion of all information held by public administrations for use by researchers and individual citizens as users or contributors to innovative projects (Renda 2016); and the EU's Directive on the re-use of public sector information, also known as the 'PSI Directive' (Directive 2003/98/EC) is now being reviewed with an aim to reduce market entry barriers, increase the availability of data, minimize the risk of excessive first-mover advantage and increasing business opportunities by encouraging the dissemination of dynamic data via application programming interfaces (APIs). Overall, this trend leads to the identification of a new strategy for the launch of innovative, disruptive platforms, which chiefly depends on making technical information available royalty-free to maximize diffusion and achieve first-mover advantage. A similar strategy is being used by Toyota for the hydrogen car[16].

Third, the open, collaborative economy is emerging in many more sectors than the often-mentioned taxi (Uber, BlaBlaCar) and hotel/accommodation (Airbnb). Owyang and McClure (2015) described already in 2015 the ever-changing landscape of collaborative economy champions as composed (based on the jargon used in Silicon Valley) by three Pegasus companies (Uber, Airbnb, Wework); a few Unicorns (Didi, LendingClub, Ola Cabs, HomeAway, Lyft, Instacart, Beepi, Blue Apron, Prosper, GrabTaxi, Thumbtack, BlaBlaCar, Etsy Tuja, Rocket Taxi); and Centaurs (Freelancer, Chegg, Rent the Runway, Postmates, Shyp, Inspirato, Circle, Hailo, RelayRides). The authors did not list the "ponies", defined as companies with a capitalization of less than 10 billion USD; and the hundreds of start-ups that have the legitimate ambition to join one of those other categories. The total capitalisation of sharing economy players calculated by the authors as of October 24, 2015 totalled 128.7 billion USD. In January 2016 a study on the 'Cost of non-Europe in the sharing economy' (Goudin 2016) placed the estimated value at €160-572 billion in annual consumption across the EU-28 (€572 billion being the highest value assessed in 2015). More recent studies however have gone way beyond these estimates: for example, Bank of America Merrill Lynch values the worldwide sharing economy at USD250b but estimates 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 economy businesses.

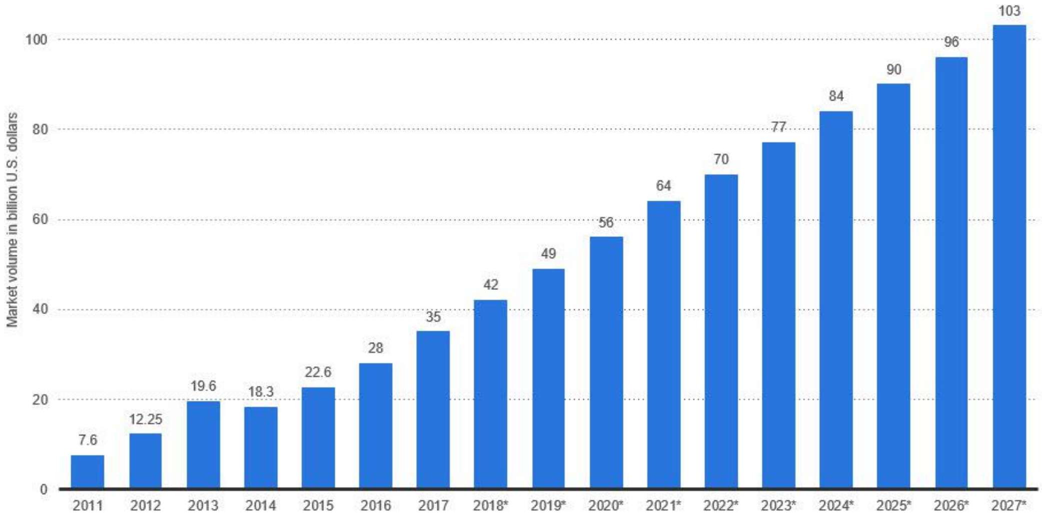
1.2.5. The data-driven economy and the rise of AI

Another important trend that bears consequences for the evolution of the ICT ecosystem is the breath-taking surge in the availability of data, coupled with the already-mentioned dramatic reduction in the cost of data storage and processing. Worldwide Big Data market revenues for software and services are projected to increase from USD42B in 2018 to USD103B in 2027, attaining a Compound Annual Growth Rate (CAGR) of 10.48%. As part of this forecast, Wikibon estimates the worldwide Big Data market is growing at an 11.4% CAGR between 2017 and 2027, growing from $35B to $103B.

Figure 7. Big Data Market Size Revenue Forecast 2011-2027 (Billion USD)

[15] http://www.digitaltrends.com/business/ford-to-open-electric-vehicle-patents-news-pictures/

[16] http://www.zdnet.com/article/toyota-pushes-hydrogen-fuel-cell-cars-with-open-patent-portfolio/



Source: Wikibon and reported by Statista.

The power of big data analytics, according to many experts, still has to be fully discovered, especially if one considers that the overwhelming majority of data available for analytics (some say, 99%) has been produced in the past two years; or, as others have observed, "the amount of data generated in two days is as much as all data generated in human history before 2003"[17]. Coupled with the already existing move towards access-based services, the use of big data can lead to important changers in the value chain of almost every sector, from retail (e.g. the "intelligent shelves") to healthcare, insurance, and even agriculture. As already demonstrated by projects such as PredPol, now implemented and adopted also in some European cities (e.g. Milan) after its first experiments in Los Angeles, also police enforcement can make extensive use of big data to improve its nowcasting abilities[18]. The list of sectors is anyway much longer, and as long as the economy is.

Big data applications are encompassing many sectors of the economy, but also many forms of innovation, including, increasingly, open innovation[19]. Powered by massive data availability, Artificial Intelligence (AI) is already being massively used in a number of areas. AI techniques include, *i.a.*, search and planning; knowledge representation and reasoning[20]; machine learning, which has led to AI breakthroughs in fields such as search and product recommendation engines, speech recognition, fraud detection, image understanding, etc.; multi-agent systems; robotics;

[17] https://www.uschamberfoundation.org/sites/default/files/Data%20Report%20Final%2010.23.pdf

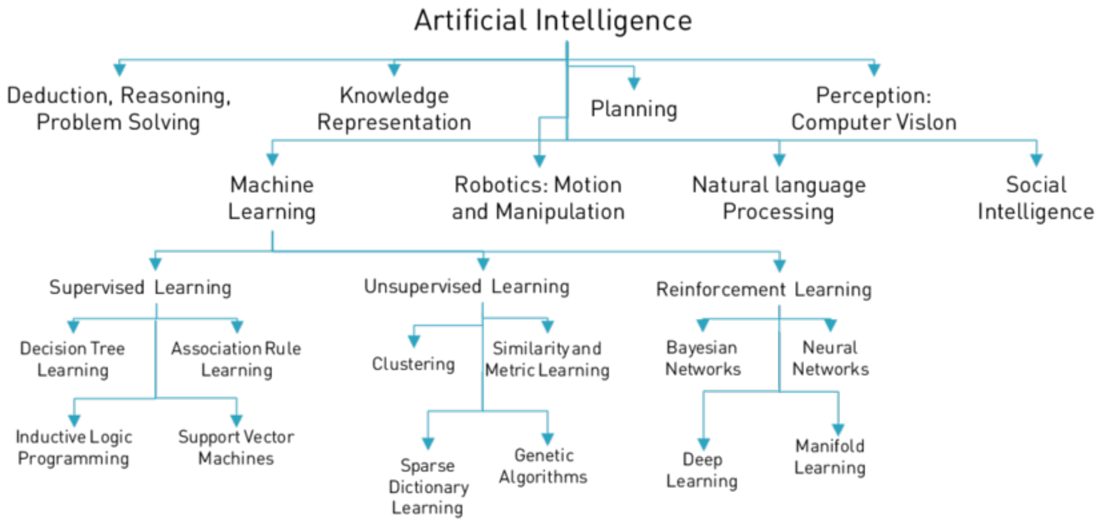
[18] See www.predpol.com for more information. For a non-technical introduction, see the article published in The Economist on predictive policy, "Don't even think about it", available at http://www.economist.com/news/briefing/21582042-it-getting-easier-foresee-wrongdoing-and-spot-likely-wrongdoers-dont-even-think-about-it

[19] The OECD (2014) reports the example of Ushahidi, a non-profit software company based in Nairobi, Kenya, which develops free and open-source software for data collection. Ushahidi's products are provided as open source cloud computing platforms that allow users to create their own services on top of it. They are free services that enable programmers to collect information from multiple sources (i.e. "crowd-sourcing") to create timelines and provide mapping services. In addition, a key component of the website is the use of mobile phones as a primary means to send and retrieve data.

[20] IBM's Watson program, which beat human contenders to win the Jeopardy challenge in 2011, was largely based on an efficient scheme for organizing, indexing, and retrieving large amounts of information gathered from various sources.

machine perception, including computer vision and natural language processing; and more[21]. In particular, Machine Learning accounts for the largest portion of current investment in AI-related R&D: it extracts patterns from unlabelled data (unsupervised learning), or efficiently categorizes data according to pre-existing definitions embodied in a labelled data set (supervised learning). Developers feed machine-learning systems large amounts of data, then the system finds the hidden relationships and uses reinforcement to improve its performance automatically. Machine learning is used *i.a.* in Google's search algorithm, digital advertising, and online personalization tools (e.g., the Amazon and Netflix recommendation engines; or the Facebook newsfeed). Machine learning also extends into quantitative processes such as supply-chain operations, financial analysis, product pricing, and procurement-bid predictions. Today, nearly every industry is exploring or utilizing machine-learning applications. Within this domain, Deep Learning uses additional, hierarchical layers of processing (loosely analogous to neuron structures in the brain) and large data sets to model high-level abstractions and recognize patterns in extremely complex data. Deep Learning has made speech understanding practical on our phones and in our kitchens, and its algorithms can be applied widely to an array of applications that rely on pattern recognition. These tools are today made available by large corporations (Google's TensorFlow, Microsoft's Control Toolkit, and many other AI tools are free and open source) and operate on common computer hardware.

Figure 8. Classification of AI approaches and domains



Source: Nazre and Garg (2015)

Combinations of these techniques have already shaken entire sectors, starting with industrial applications (e.g. for predictive maintenance) and online platforms, from e-commerce to online search, the collaborative economy and interactive online advertising. A good example is Google search, which introduced innumerable new AI-enabled functions in its first 20 years of existence (Renda 2015). Similarly, Netflix today reportedly earns as much as USD 1 billion thanks to its recommendation engine, which shows users movies they could be interested in, based on previous

[21] Some of the most sophisticated AI systems use a combination of these techniques: for example, the AlphaGo program that defeated the human champion at the game of Go used multiple machine learning algorithms for training itself, and also used a sophisticated search procedure while playing the game.

choices[22]. And Amazon invests enormous amounts of money in AI R&D to sharpen its business model and provide a more effective service to its customers. Apple, Amazon, Microsoft, Google also compete for the future of search, through their vocal assistants that make the most of recent breakthroughs in natural language processing. All this shapes a world in which information is potentially easier to find, cheaper, and more abundant.

That said, use cases are quickly emerging in many specific sectors, beyond the Internet economy. These include *autonomous transportation*, which will soon be commonplace and, as most people's first experience with physically embodied AI systems, will strongly influence the public's perception of AI; *home/service Robots*, which have already entered people's houses, primarily in the form of vacuum cleaners such as Roomba; *healthcare*, where there has been an immense forward leap in collecting useful data from personal monitoring devices and mobile apps, from electronic health records in clinical settings and, to a lesser extent, from surgical robots designed to assist with medical procedures and service robots supporting hospital operations; *entertainment*, with a huge industry investing in new exciting interactive videogame experiences; and *education*, with considerable progress expected in online learning, conversational chatbots and interactive machine tutors. AI can also potentially help development and cooperation by empowering low-resource communities, and by enabling more effective policing and, more generally, public safety.

From the perspective of regulators, AI is having far-reaching impacts on most layers of the technology stack. 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. Chen (2016) estimates the cumulative economic impact of AI from 2016 to 2026 as lying between $1.5 and $3 trillion (0.15 to 0.3 percent of global GDP). Furman and Seamans (2018) review some of the most interesting literature on the impact of AI on the economy, which mostly finds that AI and robotics have the potential to increase productivity growth but may have mixed effects on labour, particularly in the short run. They also conclude that many economists believe that "AI and other forms of advanced automation, including robots and sensors, can be thought of as a general purpose technology (GPT) that enable lots of follow-on innovation that ultimately leads to productivity growth"; the fact that AI has not (yet) translated into large productivity gains, according to Brynjolfsson, Rock and Syverson (2017), is due to a "lag between technological progress and the commercialization of new innovative ideas building on this progress which often rely on complementary investments": such lag, these authors claim, is particularly notable in the case of GPTs. This, of course, does not mean that AI is destined to succeed in no time.

As a general-purpose family of technologies, AI will pervade all sectors of the economy, and all aspects of professional and daily life. At the same time, it will have to be used responsibly: many commentators also argue that AI, if badly governed, can represent an existential risk for our society; whereas others observed that AI can make catastrophic events such as a nuclear war more likely. While this threatening narrative should not overshadow the positive disruption that AI will bring to our future society, it is important to map possible risks, which will be as essential as opportunities in forming the basis for future AI policy and regulation. As a matter of fact, while biases already exist in society, the use of algorithms may in some cases exacerbate bias, amplify it, or create it *de novo*. The use of AI-enabled algorithms, as will be explained below in Section 2, can disrupt many

[22] Carlos A. Gomez-Uribe and Neil Hunt, "The Netflix recommender system: Algorithms, business value, and innovation," ACM Transactions on Management Information Systems, volume 6, number 4, January 2016.

existing regulatory approaches, leading to potential gaps on the side of liability, consumer protection and the protection of fundamental rights.

1.2.6. Distributed Ledger technologies as emerging platform types

As already mentioned, when the World Wide Web was created its fathers decided to shape it as a fully decentralized network of networks, with no intelligence at its core. However, as the amount of information stored on the Web started to grow exponentially, reaching what is now called the "zettabyte age", the purely decentralized structure of the Internet started to change. Herbert Simon's prophecy, according to which "a wealth of information creates a poverty of attention", fully materialized on the Internet: those players that managed, over time, to conquer the attention of end users become almost unavoidable intermediaries, due to their ability to organize over-abundant information and make it available to end users in a more digestible, increasingly user-friendly way. The rise of superstar companies such as Google, Facebook, Amazon, Apple, Twitter, Netflix led, over time, to a gradual reshaping of the internet, much richer, much more user friendly, but also arguably less "neutral". Rather than dis-intermediation, the Internet led to a re-intermediation of many services: and the rise of content delivery networks, "as a service" offerings and AI-enabled applications such as recommendation engines and personalized ads led to the emergence of a new, gigantic machine in which the attention of end users, powered by network externalities, was monetized through the sale of advertising spaces (Google, Facebook), the exploitation of massive economies of scale and recommendation engines (Amazon, Netflix); or the creation of hardware-software proprietary empires (Apple). The "attention merchants" (Wu, 2017) very often re-propose an open environment where their APIs are used, in an almost-permissionless way, by third party developers who want to market their compatible apps to the billions of end users that use this fistful of platforms. The re-intermediation effect was so massive that Apple and, immediately afterwards, Amazon reached unprecedented levels of capitalization this year, becoming the first "trillion dollar" companies (and by no means the last) ever existed[23].

While this process was ongoing, in 2008 an obscure personality known as Satoshi Nakamoto revived the hopes and enthusiasm of those that dreamed about a dis-intermediated internet by proposing a decentralized ledger architecture for the realization of seamlessly interoperable transactions, known since then as the Blockchain, and supporting the use of a crypto-currency known as Bitcoin[24]. The idea behind the Bitcoin was to create a decentralized electronic transaction system, in which individuals could store and transfer value between one another without the need for central authorities. The title given by Nakamoto to its 2008 paper already clarified that the technology underlying Bitcoin reproduced the same peer-to-peer features of many other technologies that had been used since the early days of the Web, such as Napster, and the early Skype (Barkai 2001)[25]. Computer engineers have long been aware of the fact that peer-to-peer technology possesses formidable features, but also limits, in particular when it comes to scalability: this is why very often they resort to alternatives to the "pure" peer-to-peer model, to embrace so-called "hybrid" peer-to-peer models often implying so-called "supernodes", or even apparent oxymorons such as "centralized peer-to-peer" systems[26].

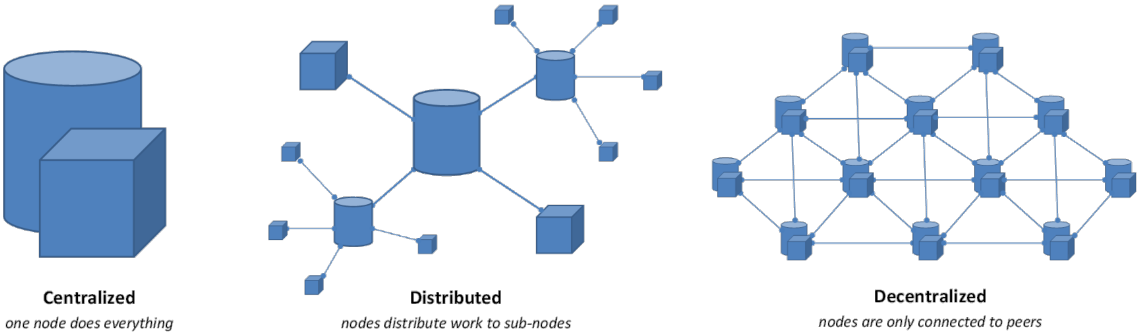
[23] https://www.cnet.com/news/amazon-follows-apple-as-second-company-to-hit-1-trillion-in-market-cap/

[24] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system (2009). URL https://bitcoin.org/bitcoin.pdf

[25] https://en.wikibooks.org/wiki/A_Bit_History_of_Internet/Chapter_6_:_Peer-to-peer

[26] In terms of architecture, a computer system can feature several organisational arrangements. It can be centralised, and as such host information and processing at the central level, without sharing the process or the information with

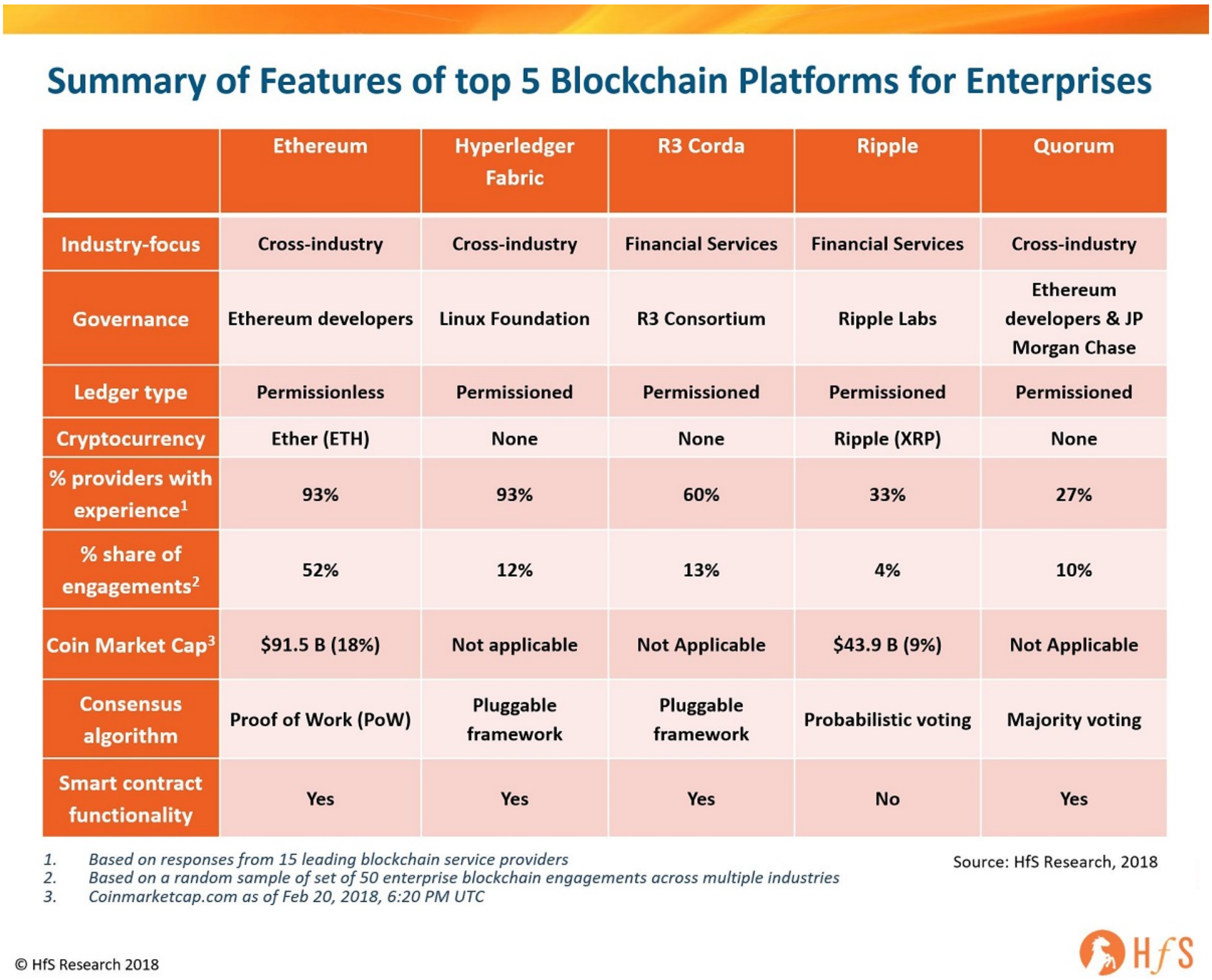
Figure 9. Centralised, distributed and decentralized computing


Centralized
one node does everything
Distributed
nodes distribute work to sub-nodes
Decentralized
nodes are only connected to peers

With the Bitcoin Satoshi Nakamoto tried to solve a specific puzzle: how to build a trustless, distributed, potentially universal digital currency by leveraging the power of cryptography to eliminate the need for trust and intermediation. The rise of bitcoins has led to the emergence of two major problems, which undermined the whole potential of Nakamoto's system: (i) the 'mining' of bitcoins and other 'cryptocurrencies' involves massive and ever-increasing computing power, which translates into extremely high energy consumption; and (ii) critics have highlighted the extreme concentration of power featured by the bitcoin. Today, distributed ledger technologies are emerging in many different forms, most often departing form the purely decentralized architecture proposed by Nakamoto in 2008. The most common blockchain-enabled systems today are not fully decentralized, as shown in Figure 10 below.

Figure 10. Summary features of top blockchain platforms for enterprises

other systems. It can be decentralized, and as such have various components that operate on local information to accomplish goals, rather than the result of a central ordering influence. A system can be federated, i.e. be a cohesive unit formed of smaller sub-units which collaborate to form the whole, but which retain significant local autonomy. Or it can be distributed, and hence be a system in which computation is distributed across components, which communicate and coordinate their actions by passing messages, and components interact with each other in order to achieve a common goal. Finally, a system is said to be peer-to-peer if it features a set of equally privileged nodes, which are equipotent participants in the pursuit of collaborative goals. The OECD (2015; 2017) has approached this issue in a slightly different way: rather than adopting a binary definition of closed versus open data, it identifies degrees of openness on a continuum ranging from closed or limited access (only by a data controller) to open and public access (figure below) to enable more differentiated approaches to data sharing and reuse. See OECD, *Going Digital in a Multilateral World* (2018).



Summary of Features of top 5 Blockchain Platforms for Enterprises

	Ethereum	Hyperledger Fabric	R3 Corda	Ripple	Quorum
Industry-focus	Cross-industry	Cross-industry	Financial Services	Financial Services	Cross-industry
Governance	Ethereum developers	Linux Foundation	R3 Consortium	Ripple Labs	Ethereum developers & JP Morgan Chase
Ledger type	Permissionless	Permissioned	Permissioned	Permissioned	Permissioned
Cryptocurrency	Ether (ETH)	None	None	Ripple (XRP)	None
% providers with experience[1]	93%	93%	60%	33%	27%
% share of engagements[2]	52%	12%	13%	4%	10%
Coin Market Cap[3]	\$91.5 B (18%)	Not applicable	Not Applicable	\$43.9 B (9%)	Not Applicable
Consensus algorithm	Proof of Work (PoW)	Pluggable framework	Pluggable framework	Probabilistic voting	Majority voting
Smart contract functionality	Yes	Yes	Yes	No	Yes

1. *Based on responses from 15 leading blockchain service providers*
2. *Based on a random sample of set of 50 enterprise blockchain engagements across multiple industries*
3. *Coinmarketcap.com as of Feb 20, 2018, 6:20 PM UTC*

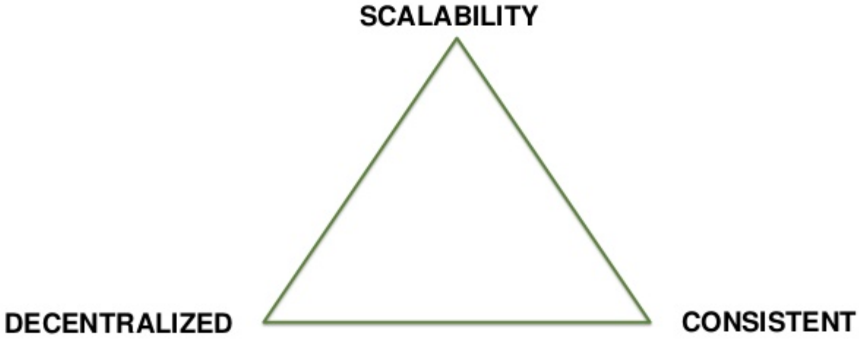
Source: HfS Research, 2018

© HfS Research 2018

Figure 11 below shows a typical representation of the "blockchain governance triangle" or DCS triangle, also known as the DCS triangle since it charts the trade-offs between decentralization, consistency and scalability. The maximum decentralization is achieved where no single entity controls the network. A blockchain is fully consistent where the network aims to keep data in sync, through real time synchronization. Scalability is maximum when performance characteristics are able to serve planet-scale or enterprise-scale needs, as typically seen in "big data" distributed databases. In this scheme, Bitcoin and Ethereum are to be located in the bottom area, due to high consistency and decentralization, but low scalability[27]. Alternative systems that aim at solving the scalability problem either compromise on decentralization (private or hybrid blockchains); or on consistency (e.g. the Inter Planetary File System).

Figure 11. The blockchain DSC triangle

[27] Both Bitcoin and Ethereum are consistent, in that all nodes see the same data at the same time. But neither Bitcoin nor Ethereum are planetary scale.



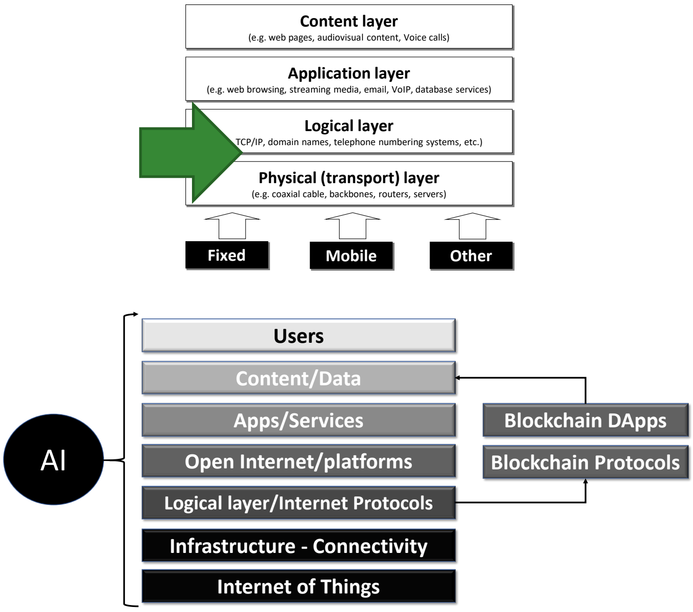
The near future will see new, and possibly successful attempts to square the circle between the three hard-to-reconcile attributes represented in the DCS triangle. As things stand, the most viable solution is to implement private blockchains in the market, but in the future hybrid or even public blockchains may become more viable. This could happen *i.a.* due to improvements in the consensus protocol, so-called sharding, independent networks/chains with "glue" connectors, or implementing "Layer 2" payment channels.

1.3. A new technology stack: emerging policy challenges

The past few years have been characterized by the rise of a new wave of technological developments, which promise to revolutionise 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 (Renda 2018; 2019). 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 12. The old v. new digital technology stack

Type the subtitle here. If you do not need a subtitle, please delete this line.


Content layer
(e.g. web pages, audiovisual content, Voice calls)
Application layer
(e.g. web browsing, streaming media, email, VoIP, database services)
Logical layer
TCP/IP, domain names, telephone numbering systems, etc.)
Physical (transport) layer
(e.g. coaxial cable, backbones, routers, servers)
Fixed
Mobile
Other
AI
Users
Content/Data
Apps/Services
Open Internet/platforms
Logical layer/Internet Protocols
Infrastructure - Connectivity
Internet of Things
Blockchain DApps
Blockchain Protocols

Source: Author's elaboration

Figure 12 above portrays 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[28]. 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 (2018) concluded that by 2030, global GDP will be 14% higher due to AI development and diffusion; the Accenture study (Purdy and Dougherty 2018) finds that growth rates will be doubled by 2035 thanks to AI. 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. Similarly, the Internet of Things is expected to massively contribute to future growth: by 2020 approximately 30 billion devices are expected to be connected to the Internet, and according to one recent forecast the number will soar to 125 billion in 2030 (IHS Markit). ARM, a big semiconductor firm recently acquired by Softbank, predicted that there will be as many as one trillion connected devices in 2035 (Renda 2018). Finally, distributed ledger technologies

[28] 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.

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.

1.3.1. Regulatory challenges of p2p architectures

The emergence of p2p architectures has had an immediate impact on regulatory frameworks, in particular for what concerns the enforcement of property rights and the attribution of liability. In the media sector, this became apparent already in the early days of the World Wide Web: while Stanford scholar Paul Goldstein predicted that the Internet would become like a "celestial jukebox", in which the possibility of charging users for each and every download and access to an information good – *e.g.* a song or a movie – would finally become reality; others, like John Perry Barlow and Eric Raymond, swiftly announced that the Internet era would have marked the death of copyright. Meanwhile, Lawrence Lessig was warning of the opportunities and dangers of using "code as law".

As a matter of fact, massive peer-to-peer (p2p) copyright infringement was made possible by the digital nature of information goods such as songs and movies ("mass without scale" effect); by the end-to-end (e2e) nature of the Internet architecture; and by the neutrality of the architecture itself. This led to the emergence of intermediaries, such as Napster, who could facilitate exchanges of copyright-protected files among peers by simply providing information on which user had the song sought by another user. Copyright law, as shaped by decades of debate and case-law in many countries around the world, was not really suited for this type of conduct. For example, in the US two doctrines were available – contributory infringement and vicarious liability. But in any event, shutting down a "facilitator" would have to pass muster under a Supreme Court precedent – the 1984 decision in *Sony v. Universal Studios*. In the Napster case back in 2001, it was quite clear from the outset that, based on these three pillars, shutting down Napster was impossible. As a matter of fact, Napster had no actual knowledge of the infringing conduct – it only kept a centralized directory, which provided only information, not files. In addition, it drew no financial benefit from the infringing conduct – no banners, no subscription fees. And it was heavily debated whether Napster could actually stop the infringing conduct in real time, if not shutting its server down. Moreover, Napster was capable of substantial non-infringing uses – sharing comments, preferences, old bootlegs, non-copyrighted recordings, making friends, etc. – and as such did not meet the Sony conditions. But it came out that, if Napster's server had been shut down, users would not have been able to engage in massive copyright infringement. It was indeed this latter issue that led the Supreme Court to decide against Napster in the end. In other words, the problem for Napster was the adoption of a *centralized architecture*.

A couple of years later, Los Angeles federal court judge Stephen Wilson opened a trial against two successors of Napster, Grokster and Morpheus. Grokster was only a very light software that connected the user to a network called FastTrack, which operated independently from Grokster and linked also other services. As a *distributed architecture*, FastTrack selected every morning some users' PCs as "supernodes", and it was supernodes that went around to look for the information to enable file-sharing, not Grokster. So, Grokster had no actual knowledge, provided no sufficient facilities for the infringing activity, and had no financial benefit from the infringing conduct. For what concerned Morpheus, it was an open source software linking users to the Gnutella network, a totally *decentralised* architecture. This sufficed for the judge to decide that the *Napster* precedent could not be easily applied. Two years later, the Supreme Court of the United States modified its approach by introducing an “inducement theory”, which bypassed the strict requirements of the applicable precedents and doctrines to impose an outcome-based rule[29]. From that day, hundreds of p2p download systems have shut down, including famous ones such as WinMX, BearShare and LimeWire[30]. However, soon after the decision, even more sophisticated systems such as BitTorrent entered the stage. Torrents display an even more decentralized architecture than Gnutella: they live a life of their own. File sharing rose by 44% between 2008 and 2014 and is expected to rise even more by 2019. In 2015, the U.S. Copyright Office stated in a report that “unlike in the Napster era, stakeholders now seem resigned to this marketplace condition and the perhaps irreversible impact it has had on the industry.”

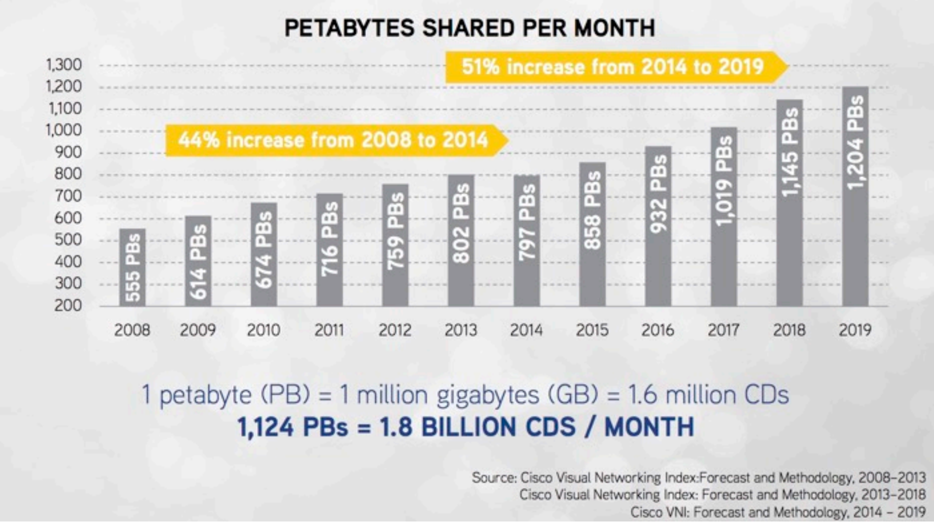
To be sure, the sustainability of the content industry improved when platforms such as Spotify, Apple Music/iTunes and Netflix started changing the business model for access to music online, from a “download to own” model to a prevalently “streaming-based” model. This form of servicification, in which access is the real product (Rifkin), deviates from the original end-to-end design of the Internet, by transforming it into a one-to-many centralized architecture, in which end users have no possibility to exchange files that belong to the platform. The Recording Industry Association of America recently reported that streaming (including paid subscriptions to services such as Spotify and Tidal, but also digital radio broadcasts and video streaming services such as VEVO) amounted to 75% of overall revenue for the record industry in the first half of 2018[31].

Figure 13. File sharing in North America (petabytes per month)

[29] *“[n]othing in* Sony *requires courts to ignore evidence of intent to promote infringement if such evidence exists. In addition to intent … the inducement theory requires evidence of actual infringement … There is evidence of such infringement on a gigantic scale. Because substantial evidence supports MGM on all elements, summary judgment for respondents was error”.*

[30] With *Pirate Bay,* Sweden has gotten as far as the US Supreme Court went in *Grokster*: it condemned the four operators of the famous website for facilitating – better, “inducing” – massive copyright infringement. And since some time has elapsed, the trial ended up capturing a technology that had been considered almost “lawsuit-proof” to date, such as the Torrent one.

[31] https://www.theverge.com/2018/9/20/17883584/streaming-record-sales-music-industry-revenue



PETABYTES SHARED PER MONTH

51% increase from 2014 to 2019

44% increase from 2008 to 2014

1 petabyte (PB) = 1 million gigabytes (GB) = 1.6 million CDs

1,124 PBs = 1.8 BILLION CDS / MONTH

Source: Cisco Visual Networking Index:Forecast and Methodology, 2008-2013
Cisco Visual Networking Index: Forecast and Methodology, 2013-2018
Cisco VNI: Forecast and Methodology, 2014 – 2019

A number of lessons can be drawn from the p2p saga on copyright infringement. First, the end-to-end architecture of the Internet, coupled with neutrality and the digital nature of media goods, is incompatible with regulatory frameworks designed for a time in which marginal costs were positive, and copying information goods led to a loss in quality. In addition, the digital economy initially evolved through flat pricing, rather than micropayments, which made the "celestial juke-box" model incompatible with social norms and consumption patterns prevailing on the Internet.

Second, by adopting a distributed or a decentralized architecture coupled with algorithms, players can distance themselves from liability, including third party liability, therefore making it very difficult for policymakers to enforce legal rules.

Third, technology is plastic. Any attempt, whether technological or non-technological, to contain or steer user behaviour online will meet with counter-action on the Web. This is typically the case when policymakers or market players try to limit the potential of the end-to-end architecture of the Internet.

Fourth, technological protection measures can be effective on the Internet, but only if they are in line with end users' behaviour, and fit existing business models. In the case of copyright, with one notable exception (the Kindle), the use of Digital Rights Management did not become the dominant way of enforcing the law, contrary to what experts and policymakers expected when the WIPO Treaty was signed in 1996, and the legislation such as the Digital Millennium Copyright Act (1998) and the EU Information Society Directive (2001) were adopted (Renda et al. 2016).

Fifth, adopting business models that deviate from the end-to-end architecture of the Internet has proven more effective, leading to the emergence of streaming services as the most important source of revenues for the content industry; however, it also comes at a price in terms of weakening communication and exchange between end users, which fosters the value of the network (so-called Metcalfe's Law).

The dis-intermediation potential of p2p technologies has become even more visible with the rise of blockchain and DLTs, and in particular cryptocurrencies. A number of challenges have emerged due to the decentralised nature of these currencies, and the potential dilution of liability emerging from the fact that decisions are either automated or adopted through consensus algorithms. The fact that DLT have no specific location creates problems in terms of jurisdiction and applicable law. Territoriality becomes challenging as each network node may be subject to different legal requirements, and there is no "central administration" responsible for each distributed ledger, the nationality of which might act as an "anchor" in terms of regulation. Relatedly, liability also represents a concern, as there may be no party ultimately responsible for the functioning of distributed ledgers and the information contained therein. Moreover, the use of blockchains creates a trust-enhancing environment among parties but does not ensure that the information on transactions stored on the ledger is true. Regulators may have to develop a legal system for recognition of blockchains as immutable and tamper-proof nodes, ensuring the veracity of information contained therein; this, in turn calls for legal rules on data protection and authenticating the identity of legal persons. At present no tribunal has issued any ruling recognizing blockchains as tamper-proof and immutable guarantees of veracity. Against this background, there is a clash has emerged between blockchain and data protection legislation, at least in those jurisdictions that grant users the "right to be forgotten" or the right to have content removed. The immutability of the blockchain is inconsistent with the possibility of removing content from the ledger, and this is leading, at least in the EU, to a reflection on how to ensure that blockchain complies with the GDPR. This is possible, *i.a.* by keeping personally identifiable information off-chain, or by using cryptographic techniques such as zero-knowledge proofs, homomorphic encryption, etc.

The use of blockchain in finance creates both enormous challenges and significant opportunities for regulators. The technology bears a disruptive potential for the whole sector, but challenges all existing intermediaries, potentially proposing a completely alternative way of organizing and enforcing transactions. This is especially true of initial coin offerings (ICOs), where cryptocurrency is issued in the early stages of a blockchain business to raise capital. Many countries are enacting separate systems to regulate cryptocurrencies and ICOs or attempting to bring ICOs under the umbrella of existing institutions through the interpretation of securities laws. For example, Korea decided to ban all forms of ICOs since September 2018 and confirmed its decision at the end of January 2019, due to fear of uncontrolled speculation and lack of investor protection[32].

The use of cryptocurrencies such as Bitcoin also led to unprecedented possibilities for money laundering, leading regulators to face a regulatory void. The US took action already in 2013 to clarify the applicability of Bank Secrecy Act provisions to cryptocurrency, whereas in Europe only after the terrorist attacks in Paris in 2015 EU ministers called for a "strengthening of controls" around cryptocurrencies, citing their potential use in terrorist fundraising and money laundering. This ultimately led to the 5th AML Directive[33]. Beyond Bitcoin and Ethereum, a good number of cryptocurrencies are already electronically traded and can be directly convertible in fiat currencies: Ripple, Bitcoin Cash, Litecoin, Stellar, Cardano, Monero and Dash.

[32] Auer and Claessens (2018): Note that only those cryptocurrencies based on permissionless, decentralised protocols are open to anyone and thus entity-free. By contrast, cryptocurrencies running on permissioned protocols give select actors special access rights. Inasmuch as those select actors can be identified, such cryptocurrencies can be identified with legal entities. See BIS (2018) for a discussion of the differences between permissionless and permissioned cryptocurrencies.

[33] Virtual currency exchange platforms and custodian wallet providers will, like banks, have to apply customer due diligence controls, including customer verification requirements. These platforms and providers will also have to be registered, as will currency exchanges and cheque cashing offices, and trust or company services providers.

Likewise, smart contracts pose challenges for regulators in terms of territoriality and enforceability. Despite their denomination, smart contracts are simply code tasked with automated decision-making in case of a specific occurrence. They are sets of instructions, rather than a legally binding contract that results from the will of two or more parties; that said, in a DLT they produce effects and regulate transactions, in a way that potentially creates an alternative legal ecosystem, not necessarily compatible with national legal systems. The issues mentioned above regarding territoriality and liability are likewise applicable to smart contracts but require a series of additional considerations: as far as jurisdictional issues are concerned, there is not only the issue of whether the distributed ledger itself has a specific location, but also the issue of signatories to the contract being subject to different laws under their respective jurisdictions. Regarding liability, numerous parties are involved in smart contracts: not only the parties to the contract, but also the creator of the same (usually some kind of encoder) and the custodian of the contract (ideally there would be no need for the latter party). As well as the obvious possibility of one of the contracting parties breaching the contract, there is a chance that the contract itself may be flawed, either due to coding errors or design errors. Thus, when a smart contract fails to work as expected, which party would be liable?

While blockchains are thought to be particularly useful for the Internet of Things, problems of territoriality and liability, including the ones related to smart contracts, can only become more evident as the ledger now includes a series of entities and nodes that are located across the globe.

The similarity of the problems raised by online p2p copyright infringement and DLTs should not come as a surprise. Indeed, Ito *et al.* (2017) recognize the parallelism by arguing that blockchain and DLTs are likely "to do to the financial system and regulation what the internet has done to media companies and advertising firms"[34].

1.3.2. Platformisation and monopolisation: antitrust and regulatory aspects

Perhaps the most widely studied challenges posed by the digital economy to traditional regulatory frameworks are those falling the domain of competition policy, including antitrust and competition-enhancing regulation, such as the regulation of network industries. The fact that the digital economy knows no borders should not only be taken in terms of territoriality: the Internet has blurred the boundaries across sectors (horizontally), and across layers of many value chains (vertically), creating an *impasse* in many regulatory frameworks.

1.3.3. Pricing digital goods and services

Since the early days of the Internet, the role of the price mechanism has gradually changed, to some extent losing its centrality in the world of regulation and competition policy. In the era of "mass customization" or both products and prices, the price level sometimes disappears from the market. Furthermore, even when they are positive, prices often take the form of blanket licenses or refers to bundled goods/services, which in turn makes it difficult to assess whether the price of a single product or service is excessive.

1.3.3.1 Emphasis on mark-up pricing is misplaced

[34] https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media/

The first, inevitable consequence of the rise in the digital economy is that all regulatory frameworks based on the observation of cost-based pricing become obsolete. Price formation in the digital economy obeys to different rules. And sometimes price does not even exist or is not expressed in monetary terms.

More specifically, regulation imposing access obligations at regulated prices clashes with the multi-sided nature emerging platforms models. The clash between mark-up pricing and two-sided markets emerged already in the late 1990s, when regulators (in Australia) and antitrust enforcers (in other parts of the world) started looking at the level of interchange fees applied by credit card circuits such as Visa and Mastercard (Evans and Schmalensee 1999): two decades of court litigation and regulatory attempts have not led to full clarity as to whether interchange fees should be set on the basis of cost, or whether they should float in order to keep the two-sided market in equilibrium: the recent, 5-4 decision of the US Supreme Court in *Ohio v. American Express* seems to have marked a move away from traditional approaches to excessive pricing.

A similar issue is now happening with network industries: apart from broadband networks, which clearly exhibit multi-sided platform characteristic (Ofcom 2005), also electricity networks are now abandoning their original "dumb pipe" features to become enablers of value-added applications in modern smart grids. Imposing cost-based pricing through traditional bottom-up or top-down regulatory models (typically relying on remunerating cost and adding the weighted average cost of capital, WACC) makes little sense in such an environment, in which prices are set as a function of indirect network externalities, rather than as a mark-up on unitary costs.

1.3.3.2 Regulatory and competition concerns with zero-price goods

It is a well-known saying that "if you're not paying for the product, then you are the product". As a matter of fact, in the digital economy price often disappears, and product appear to be available entirely free of charge to their end users. This happens due to a number of possible factors.

First, in multi-sided markets price can often drop to zero or even be negative as a means for platform operators to balance the different sides of the market. This is the case for cardholder fees in some credit card circuits: placing them at zero and charging more on the merchant or the interchange fee can be a way to ensure that the business model is sustainable.

Second, in advertising-based business models (e.g. Google, Facebook) free access to services and content often hides a non-monetary payment: users simply contribute their attention, in what has sometimes been terms as "competition for eyeballs" (Renda 2015).

Third, even when no online advertising is possible on a platform, end users often "pay" services online by contributing their personal data and enabling online intermediaries to capture enormous value from seemingly free transactions. This, in turn, creates a number of challenges in regulatory policy: from privacy protection to the taxation of profits (since value is often created in legal systems where large intermediaries are not legally established), to the issue of fair distribution of revenues and even fair remuneration of work.

The OECD (2018) has studied possible dimensions of competition in case of zero-priced markets, recognising that there are potential legal hurdles associated with capturing zero-price markets under competition laws in some jurisdictions, and identifying. Four main dimensions of competition over quality in zero-priced markets: privacy and data security, advertising content, ease of switching and choice associated with complements. Some of the key recommendations include an enhanced focus on quality "as a measure of the terms of the exchange between firm and customer", avoiding too rigid market definition, and tackling consumer behavioural patterns associated with zero-price goods that may lead to adverse market outcomes.

1.3.3.3 When price disappears: ushering the era of price-adjusting al personalized pricing

There are at least two additional reasons that explain the increased uncertainty faced by regulators with respect to the price mechanism in the digital economy.

On the one hand, the increased reliance on dynamic algorithms by retailers, especially in the e-commerce domain (where reportedly two third of retailers use such algorithms in Europe) makes it very difficult for regulators and competition enforcers to distinguish competitive price levels from anticompetitive (i.e., collusive) ones. After the initial contribution of Stucke and Ezrachi (2016), competition authorities have started to look at the use of algorithms to facilitate and enforce collusive agreements (CMA 2018). In June 2017 the OECD held a roundtable on "Algorithms and Collusion" as a part of the wider work stream on competition in the digital economy, in order to discuss some of the challenges raised by algorithms.

In addition, concerns for regulators emerge also since large platforms such as Amazon and Uber often use forms of peak or "surge" pricing, which have unpredictable effects on consumer welfare. For example, in early 2016 an Uber customer sued Uber CEO Travis Kalanick alleging a price-fixing conspiracy. The substance of the complaint was that since Uber does not employ its drivers, its price-setting, and specifically its price coordination through surge pricing, amounts to a violation of the Sherman Act, whether through a multilateral conspiracy or through unilateral action. In other words, if Uber is not an employer of its drivers under labour law, then it should not be able to set and coordinate prices among those independent contractors and evade liability under antitrust. The case was later dismissed in court, but a class action is still pending.

Moreover, antitrust authorities and scholars have focused on the practice of personalised pricing, which tailors the retail price to specific characteristics related to the end user, such as the IP address, the time spent browsing the Web, and also more personally identifiable information that can be useful to infer the user's maximum willingness to pay and adjust the price accordingly. A recent report by the UK Competition and Markets Authority tests the UK market for evidence of personalised pricing, however finding limited evidence of the widespread use of algorithms for this specific purpose[35].

1.3.4. Antitrust, regulation and the elusiveness of market power

The digital economy challenges the approach of regulators to market power and related policy frameworks. Traditionally, antitrust has relied on a series of proxies to challenge significant market power: from the definition of the relevant market to the assessment of market shares and tools such as the SSNIP test, there are countless practices in antitrust that are challenged by the peculiar economics of the digital economy.

1.3.4.1 Antitrust in the digital economy

The application of competition rules to the digital economy has proven to be problematic since the early days of personal computing. The *Microsoft* saga in the United States and later in many other

[35] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746353/Algorithms_econ_report.pdf

jurisdictions uncovered many of the structural challenges that antitrust faces: such challenges are more related to the proxies used to implement and enforce antitrust, as well as to the "pacing problem", than they are to the overarching principles of antitrust law. The latter indeed remain largely relevant in the digital economy.

First, when it comes to the definition of the relevant market, very often antitrust authorities have faced significant trouble. Antitrust analysis indeed requires that the possession of significant market power is analysed with respect to a 'relevant product market', defined as the group of products or services that are sufficiently substitutable with the one at hand, from a demand-side as well as from a supply-side perspective.[36] The relevant product market is thus the group of those products and/or services that "are regarded as interchangeable or substitutable by the consumer, by reason of the products' characteristics, their prices and their intended use".[37] In addition, a '**relevant geographic market**' has to be defined, namely "the area in which the undertakings concerned are involved in the supply and demand of products or services, in which the conditions of competition are sufficiently homogeneous and which can be distinguished from neighbouring areas because the conditions of competition are appreciably different in those areas".[38] Based on these definitions, it seems clear that the relevant market would need to comprise products that are broadly similar.

Reality, however, suggests that **market definition in certain high-tech settings is likely to prove much more complicated and controversial than in more traditional markets.**[39] Already in the 1990s the Microsoft saga in the United States showed that in markets dominated by network externalities and learning effects, which tend to feature winner-take-all competition and 'tipping' effects, the definition of the relevant market can prove very difficult, and sometimes of limited use.[40] In addition, the choice of tools such as the "Hypothetical Monopolist test" or "SSNIP test" is of little use when prices are hidden, zero, or even negative. From a more academic perspective, as a result of network effects and Schumpeterian competition, the history of the Internet shows that competitive pressure is seldom exerted by players that are already present in a given relevant market; on the contrary, competition sometimes comes from other existing markets and most often from future products or platforms (as in the case of Navigator for Windows). It is this type of competitive pressure that most effectively disciplines successful players: the urge to compete to survive is not put to rest, on the Internet, by the mere fact of having conquered a stronghold in a province of an ever-changing ecosystem. Some authors have suggested a **'follow the money' approach** to market definition, which would entail that the Commission gives up the definition of an 'online search'

[36] See the European Commission (1997), "Notice on the definition of relevant market for the purposes of Community competition law", *Official Journal* C 372, 9.12.1997, pages 5–13.

[37] Id. §7.

[38] Id. §8.

[39] See Abramson, B. (2008), "Are "Online Markets" Real and Relevant? From the Monster-HotJobs Merger to the Google-DoubleClick Merger", 4 *J. Competition L. & Econ.* 655 (2008). And Ratliff and Rubinfeld, *supra* note 43.

[40] See Pardolesi and Renda (2004), *supra* note 5. For example, in the antitrust case concerning Microsoft's alleged anticompetitive tying of Windows with Internet Explorer, the US antitrust authorities had problems identifying the relevant market, since competition was occurring between two products that were far from interchangeable in the strictest sense of the word: an operating system and a browser do not perform the same functions, but they could still be competitors because the browser (Netscape Navigator) could be seen as a future platform for applications (thanks to the Java programming language), potentially replacing Windows as the *de facto* industry standard, i.e. the most prominent multi-sided platform available to end users and application developers. This triggered Microsoft's reaction, described as 'defensive leveraging': but already at that time, the fact that Microsoft could be described at one and the same time as a quasi-monopolist and a fierce competitor raised many eyebrows among academics.[40] In 1999 the FTC faced an even clearer *impasse* when it defined Intel as a monopolist in the production of Intel processors.[40] Also the European Commission made a very questionable use of market definition in its Microsoft decision in 2004, by identifying a market for entry-level workgroup server operating systems that was very difficult to justify in antitrust (and economic) terms.[40] Since then academics and practitioners have increasingly questioned the usefulness of market definitions, especially in high-tech markets, and especially whenever the market at hand features dynamic competition between multi-sided platforms.

market in favour of the relevant market for online advertising: this would imply the inclusion of players such as Facebook in the relevant market.[41] Another alternative is that the competition authority decides to skip market definition altogether, as suggested recently by some scholars, and concentrate on identifying sources of competitive pressure that might exert a disciplining effect on the allegedly dominant company.[42]

Just like market definition, also the assessment of dominance has its own established tradition. And just like market definition, **the assessment of dominance has run into trouble with the advent of the Internet era**. In particular, competition authorities and courts typically define dominance with reference to a company's ability to behave independently of competitors, customers, suppliers and consumers. In practice, however, such assessment typically relies on market shares as a first indication of the possession of market power. Since in the digital economy, network externalities often lead to market tipping, market shares will most often show the presence of a dominant company, even if when market is highly contestable. In settings characterised by 'tipping' and competition 'for' the market, the observation of market shares is unlikely to fully account for the existence of contestability and the threat of future entry. To quote i.a. Rubinfeld and Hoven (2001): "Many network industries are dynamic, in which case the market is a moving target, evolving as technology changes in response to innovation. Antitrust analysis must occasionally focus, therefore, not only on static competition within the market as it is currently constituted, but also on dynamic competition for the market of the future, that is, competition to control the next market standard (if there is one)."[43] This, of course, does not mean that market shares are entirely useless as a proxy for market power: the view that market shares should be abandoned altogether has been authoritatively criticised as too extreme in the literature.[44] However, there is consensus on the fact that **'Schumpeterian' competition calls for increased attention for the competitive conditions of the market under analysis, including competitive pressure exerted by alternative platforms.**

Furthermore, in the digital economy the **appraisal of the effects of allegedly anticompetitive conduct becomes very tentative and ultimately controversial**. For example, if competition authorities consider the elimination of competition as a cause of consumer harm (due to lack of product variety and consumer choice), then tipping markets with winner-take-all competition may often be found to host anticompetitive conduct[45]. If consumer harm is interpreted as a consequence

[41] For a preliminary discussion of this issue, see Van Gorp, N. and O. Batura (2015), *Challenges for Competition Policy in a Digitalised Economy*, Report for the European Parliament, at http://www.europarl.europa.eu/RegData/etudes/STUD/2015/542235/IPOL_STU(2015)542235_EN.pdf

[42] See Kaplow, L. (2010), "Why (Ever) Define Markets?", 124 *Harv. L. Rev.* 437 ("This Article advances the immodest claim that the market definition process is incoherent as a matter of basic economic principles and hence should be abandoned entirely"). Werden, G. J. (2012), "Why (Ever) Define Markets? An Answer to Professor Kaplow", at SSRN: http://ssrn.com/abstract=2004655 ; and later Kaplow, L. (2012) "Market Definition Alchemy", 57 Antitrust Bull. 915 (2012).

[43] See Rubinfeld, D., and J. Hoven (2001), "Innovation and Antitrust Enforcement". in Ellig, J. (ed.) *Dynamic Competition and Public Policy: technology, innovation, and antitrust issues*. USA: Cambridge University Press, 2001. See also Evans, D.S. and R. Schmalensee (2008). "Markets with two-sided platforms?", *Issues in Competition and Law and Policy* (ABA Section of Antitrust Law) 1 (28), 667–693.

[44] Katz, Michael L. and H. A. Shelanski (2005), "'Schumpeterian' Competition and Antitrust Policy in High-Tech Markets". *Competition*, Vol. 14, p. 47, 2005. Available at SSRN: http://ssrn.com/abstract=925707

[45] For example, in the first Microsoft case (launched by the FCC for tying of MS-DOS with Windows back in the early 1990s), the key issue was whether Microsoft had innovated by adding a product to its OS, or whether the dominant effect was harm to its competitor Novell, which was not in a position to fully replicate Microsoft's integrated offer. Already at that embryonic stage, the issue was whether antitrust should place incentives on competitors to build their own killer app (just like Microsoft had done with Windows), or whether antitrust should force successful companies to refrain from tying products, and offer the same bundling possibility to its rivals. The latter option (allowing Novell to offer Windows on its DR-DOS) would probably mean reducing Microsoft's incentives to innovate in the future, and offering Novell the possibility to free ride on Microsoft's innovation. Either solution would thus have led to pros and cons: in the end, the shortcomings did not materialise for Microsoft due to the fact that, by the time the investigation was closed (with a consent decree), the company has already had the time to consolidate its market position and market share to the detriment of its only rival. A few years later, the Microsoft-Netscape dispute was largely approached with attention to the

of monopoly power leading to price increases, antitrust authorities will be unlikely to find instances of harm in contexts where prices are sometimes invisible, and often zero. The potential consideration of lack of innovation as consumer harm is also difficult, since most of the large tech giants on the Internet invest huge amounts in R&D despite their large market shares (if measured with the traditional antitrust market definition tools). Over the past two decades, a wealth of economic literature has demonstrated that companies in many high-tech markets compete for the future, and consistently that competitive pressure also comes from future players. If one concedes that the companies that legitimately win a competitive race will enjoy high market shares for a limited period of time to the detriment of the losing players, it is difficult to imagine that the same company could be charged with anticompetitive conduct for the same reason, and the same behaviour. Accordingly, many scholars have observed that the real antitrust concern lies in so-called 'monopoly maintenance' strategies, especially when such strategies create a straight-jacket effect on innovation.

Finally, finding suitable remedies for identified violations is also very problematic. Past competition cases in the digital economy are already fraught with remedies of very limited effectiveness: these include, at the EU level, the so-called 'stripped-down' version of Windows (without the Media Player), an unbundling remedy that proved totally ineffective; the 'ballot screen' remedy imposed on Microsoft during the *Opera* case, which was only marginally important in the reshuffling of the browser market that was brought about by technological evolution and the emergence of new products;[46] and the three rounds of commitments proposed by Google in its attempt to settle the issue with the European Commission, which ended up being rejected by Google's own competitors. Difficulties in monitoring the condemned undertaking's conduct have led competition authorities to even consider using blockchain for enforcement purposes (OECD 2018)[47].

1.3.4.2 Should antitrust enforcers be stricter on proposed digital (data-driven) mergers?

While it is increasingly acknowledged that the digital economy significantly affects the viability of traditional antitrust tools related to single-firm conduct, as well as those applied to cartels, a body of knowledge is emerging also with respect to the peculiarity of the digital economy when it comes to merger control. Here too, the assessment of unilateral and combined effects requires in-depth knowledge of the peculiar dynamics of competition in many digital economy markets. The absence of overlaps between relevant product or geographic markets, which normally leads antitrust authorities to consider a merger as unlikely to create competition concerns, requires additional scrutiny exactly since competition, in many provinces of the Internet economy, often emerges between players that operate in different relevant markets.

Mergers in the digital economy have raised the attention of scholars for at least two reasons. First, the relevance of the acquisition of additional customer data in so-called data-driven mergers seems to create a whole new dimension of non-price effects, which should be carefully appraised by antitrust authorities. Recently, the German and French Competition Authorities issued a joint

disadvantage caused by Microsoft to Netscape through a contractual and later technological tying strategy: no sufficient attention was devoted to the positive externalities that had been generated by Windows for Navigator: the mere existence of windows had been a key precondition for the success of Netscape Navigator.

[46] See i.a. Manne and Wright (2012), showing that "The changes in Internet Explorer's market share in Europe almost perfectly mirror its changes worldwide, and differ only slightly from changes in its US market share, demonstrating that its declining share of the European market cannot be attributed to the browser choice screen". The authors show also complementary evidence that Chrome's market share increased almost identically in Europe, in the United States, and worldwide, despite the operation of the ballot screen in Europe.

[47] http://www.oecd.org/daf/competition/blockchain-and-competition-policy.htm

report on Big Data, which observes that merged entities could acquire knowledge of customers' preferences that rivals may not be able to match. As observed i.a. by Linskay (2018), "such consolidation of market power can be of relevance to data privacy if it enables the monopolist to exploit consumers by imposing unfair terms and conditions on them, or by exerting downward pressure on competition on the basis of data protection"[48]. Scholars have observed that past evaluation of mergers such as Google/DoubleClick, Facebook/WhatsApp and Apple/Shazam have not fully considered this aspect of the merger's effects.

Second, the literature is split between pro-competitive views of digital mergers, which claim that they facilitate innovation by offering SMEs an easier "exit" through acquisition by larger companies; and anti-competitive views, which focus on so-called "pre-emptive mergers": among others, Van Gorp and Batura (2015) discuss this issue, arguing that "paranoia may also stimulate large firms to go on shopping sprees with intention to eliminate potential disruptive innovators"[49]. When companies decide to acquire a smaller player that has even a small potential to turn into a maverick and later a future platform, they are consolidating their position in a way that competition authorities, through standard parameters, would not be able to spot.

Against this background, there seems to be room for a tailoring of merger appraisal to the specifics of competition in the digital economy, especially when data hoarding is a possibility post-merger, but also more generally when the risk of elimination of a future competitor is high despite the lack of significant overlapping effects in the merger, and also when the turnover of the acquired company appears to be low: not surprisingly, in the digital economy companies can develop a very promising business model without necessarily selling their services for a positive price: as observed by Van Gorp and Batura (2015), "the question is how to measure the size of a firm. Turnover is not a practical metric because some firms may make minimal turnover (like WhatsApp). Given the importance of scale economies and network effects, a better metric would be the number of users together with an estimation of the size of the network effects".

1.3.4.3 From antitrust to regulation (1). Network industries and "Open API" regulation

All the above-mentioned problems created by the digital economy to antitrust enforcers reverberate, inevitably, on those regulators that apply a competition-oriented framework in their daily activities. This is certainly the case for many regulators in network industries, which often apply regulatory frameworks that are chiefly based on the finding of market power and the consequent introduction of mandatory regulatory remedies such as network-sharing obligations. In some cases, this is very explicit: for example, the EU regulatory framework for electronic communications is based on a same notion of "significant market power" (SMP) that is equated with the notion of dominance under EU antitrust rules.

Not surprisingly, the first problems emerged in electronic communications, due to the fact that fixed and wireless broadband networks support the digital economy with all its applications and services (this is the physical layer described in figure 10 above). When so-called "over the top" players such as Skype, Vonage, Google Hangout or Apple FaceTime started to compete with infrastructure players operating in the e-communications domain, it took years for regulators to adjust their market definition and finding of market power. And this led to paradoxical situations in which mobile network operators were found to be dominant under e-communications regulation, but at the same time were considered to be the weaker player by competition enforcers when dealing with

[48] https://one.oecd.org/document/DAF/COMP/WD(2018)70/en/pdf

[49] http://www.europarl.europa.eu/RegData/etudes/STUD/2015/542235/IPOL_STU%282015%29542235_EN.pdf

Apple iOS and Google Android. Today, the appraisal of market power in e-communications cannot ignore the lack of independent behaviour of many operators, who significantly depend on the platforms they offer to their customers. The decision to force infrastructure-owning operators to share their networks with new entrants strongly depends on whether these operators are found to be competing with players such as Skype, as well as whether they are found to hold any bargaining power vis à vis OTT players.

This similar *impasse* is about to be replicated in other network industries, such as electricity. While in 2002 Tim Wu, in introducing the concept of network neutrality for e-communications, used electricity as example of the quintessentially neutral network, today so-called grid neutrality has become a well-known policy issue in electricity[50]. In the age of smart grids, electricity networks are indeed undergoing a process of platformisation similar to the one that affected e-communications more than a decade ago. And the problem of "grid neutrality" has now become a key policy issue to ensure a level-playing field between service providers in the over-the-top electricity world[51].

Beyond network industries, a corollary of the platformisation of traditional markets is the ongoing transition from physical access regulations (such as network-sharing obligations, or compulsory IP licensing of Standard Essential Patents at FRAND conditions) to virtual, information-based liberalization policies. For example, in the financial sector lawmakers are now asking banks to open up their Application Programming Interfaces (APIs) just like Microsoft was asked to do by antitrust authorities in the late 1990s and early 2000s. In particular, the revision of the EU Payment Services Directive (PSD2) imposed the opening up of APIs (in this case, containing their customers bank history) to enable new entrants to develop value added Fintech services[52]; at the same time, the new Directive was criticised for potentially putting in the hands of large tech giants additional data, without imposing on them any reciprocal data sharing obligation. This, in turn, has led to the emergence of regulatory proposals to mandate data-sharing on the side of large tech conglomerates.

1.3.4.4 From antitrust to regulation (2). Creating a level playing field "across layers": network neutrality and the collaborative economy

At the intersection between antitrust and regulation, the layered stack of the Internet economy often creates challenges related to the establishment of a common, level-playing field between players with completely different business models. For example, the network neutrality saga started as a problem of competition between the physical and the application layers of the Internet, and then evolved into a much bigger issue of freedom of speech and end user protection in cyberspace. This unravelled a typical problem of tackling cross-layer problems through sectoral policies: that regulators end up focusing on the domain in which they are competent to regulate and forget to observe the bigger picture. And they are sometimes led by an optical illusion: that a sound competitive environment can be created by imposing neutrality obligations at one layer only. In my past research (Renda 2014), I have renamed these problems as the "Keys and Lamp post" syndrome, and the "Trabant Syndrome".

[50] "The electric grid does not care if you plug in a toaster, an iron, or a computer ... [It's] a model of a neutral, innovation-driving network" (Tim Wu, 2002).

[51] https://www.vox.com/2015/10/9/9483803/grid-neutrality; https://onlinelibrary.wiley.com/doi/full/10.1002/gas.21976

[52] Directive 2015/2366/EUof the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

In the case of network neutrality, the initial policy discussion was based on the idea that wireline and wireless network operators would be able to exert superior bargaining power vis à vis over the top players wishing to offer services to end users. Accordingly, most of the regulatory or soft law measures adopted since the early 2000s in various jurisdictions were mostly aimed at avoiding abuses of market or contractual power on the side of Internet Access Providers; however, the platformisation of the Internet soon created a situation in which OTT players hold as much (or even greater) contractual power vis à vis IAPs; in addition, these players make regular use of other means to accelerate traffic, such as caching services and Content Delivery Networks; and finally, the increased use of AI in online platforms to filter out spam, rank and select content (e.g. in online marketplaces, app stores, and search engines) led to regular, inevitable discrimination between bits flowing on the Internet. The result of these technological developments was a deadly blow to the initial theoretical foundations of network neutrality regulation. First, it became clear that mandating network neutrality by regulating would not make the Internet neutral (Renda 2015). Second, it led to the inevitable conclusion that neutrality at all layers of the Internet is neither possible, nor desirable, and this is leading to a paradigm shift in the regulation of Internet intermediaries, initially shielded from responsibility for the content flowing on their supposedly "dumb pipes" (or "mere conduits"). And third, it shifted the attention towards discriminatory practices at the level of online platforms, where they were subject to careful study and some initial regulatory measures over the past years (see next Section).

Similarly, the rise of the collaborative economy has created a bridge between the application layer of the Internet and traditional markets such as local transportation, food catering and hospitality services. As mentioned i.a. by Hatzoupoulos and Roma (2018), the collaborative economy facilitates the connection between peers, while bypassing the traditional economic intermediaries. The peculiarities of the Internet, in particular the end-to-end nature of the network and the consequent direct network externalities, have made sharing possible at a previously unattainable scale, just as occurred in the above-mentioned case of Napster. As observed in a recent contribution by Erixon and Sorensen (2016), the sharing economy creates various challenges for traditional regulatory frameworks. First, in terms of **labour relationships** (as already mentioned above with respect to Uber's surge pricing) these platforms are typically reliant on contractual relationships with participants that, rather than employees, are involved as micro-entrepreneurs: this can lead to situations in which participants are exposed to "greater risk, reduced benefits and lower job security", a situation that called for regulation in a number of countries (De Stefano, 2016)[53].

Second, information asymmetries due to the relative anonymity of participants, and relative lack of **trust in the system**, have led platforms to adopt diffuse bilateral rating systems. But the "rating economy", in and of itself, can be problematic in many respects. As a matter of fact, ratings can be rather obscure, are easily manipulated (Lee, 2015), can be too simplistic (Parigi et al., 2013), and in some cases can be intrusive of participants' privacy.

Third, especially in crowd-working platforms **legal liability** is often placed on participants and users themselves. Erixon and Sorensen (2016) observe that platforms like Lyft or Uber require that participants have their own driver's license and insurance, and in some countries require criminal

[53] In the UK, two Uber drivers, James Farrar and Yaseen Aslam, took Uber to court in 2016 in a bid to become recognized as Uber employees or workers under UK employment law, rather than as independent contractors or self-employed (*Aslam and Others v Uber BV and Others*). The court decided that they should be characterized as workers. This meant that Uber drivers can receive some but not all of the benefits and job security of regular employees. In its justification, the court has generally rejected Uber's use of multiple corporate personalities to circumvent the relevant UK employment and competition laws (OPBP 2017: 6). See various CEPS report on the conditions of platforms workers in specific sectors, at https://www.ceps.eu/topics/platform-economy.

records and other status checks; whereas Airbnb requires that participants purchase home insurance, and do not carry out health and safety inspections, rather encouraging hosts to install smoke or carbon monoxide gas detectors for which they do not require proof. All this leads to a massive shift in liability from the platform to individual participants, with what Erixon and Sorensen (2016) define as “obvious public interest implications that have not yet been adequately addressed, either by the platforms themselves or by national legislators”.

Fourth, and more generally, the **bargaining power of participants vis à vis the platform in many of these collaborative economy services appears to be fairly limited**: depending on the possibility to multi-home and on the overall competitive landscape of the market, there may be very little choice for participants than to rely on the platform, thereby ending in a position of lock-in. This leads to situations that mirror closely cases of superior bargaining power, abuse of economic dependency or abuse of “relative dominant position” that have been tackled, in other sectors, by many legislators around the world, especially in Continental Europe (Renda et al. 2012; Kalff and Renda forthcoming). In many countries, competition authorities have started to take a closer look at the sharing economy as a phenomenon that potentially shakes the foundations of competition law, calling for careful monitoring of “the possible imposition by sharing economy dominant providers of rules that favor exclusivity, or single-homing, to their platforms” (Muscolo 2018; King 2015).

Finally, the bottom-up, end-to-end, unlicensed and unregulated nature of collaborative economy platforms has led to situations that are similar to the so-called **“tragedy of the commons”** theorized by Garrett Hardin (1968), i.e. cases in which the absence of clearly defined usage rights lead to over-exploitation of a given asset or system. In the case of ride-hailing, some countries have experienced an over-proliferation of platforms and brands, with consequent excess supply of vehicles and difficulties in pedestrian mobility due to unregulated and uncontrolled parking.

Regulatory authorities have faced significant challenges in their attempt to regulate the collaborative economy. The **uncertain legal classification** of these platforms (e.g. is Uber a transportation service provider, despite the fact that it does not own any vehicle and its drivers are not employees?) has made it very difficult to establish a level playing field with more traditional players. Accommodating these services in the same market also creates more direct regulatory problems such as attributing responsibility for **universal service provision** (e.g. serving remote rural areas; taking on board disabled passengers). And in some cases, the disruption brought by these services, coupled with differential regulatory treatment, has led to the loss of expected revenues (e.g. from taxi licenses) for incumbent players, which some legal systems are now trying to address in various ways, including by proposing *ad hoc* compensation schemes[54]. In some cases municipalities have chosen to directly ban these services, whereas in other jurisdictions complex negotiations have led to a direct regulation of the platforms.

1.3.4.5 From antitrust to regulation (3): unfair trading practices between platforms and businesses

The pressure to tackle the perceived prominence of large online platforms through antitrust means, as already mentioned, ended up clashing with the difficulty to adapt traditional tools of competition policy to the different competition dynamics of online markets. In particular, many of the conducts observed in online markets appeared to be independent of the existence of a dominant company

[54] Medallion prices, which reflect the value of running a taxi fleet, have felt the impact of Uber: the average price of New York medallions has suffered a 17% decline since a peak in 2013, with Chicago and Boston observing declines of 17% and 20%, respectively (Barro, 2014; Chang 2015).

in a given relevant market, but were rather related to the differences in bargaining power in commercial relations between a platform and the businesses that rely on it to reach their end users. These conducts, which often take the form of potentially unfair commercial practices, are very similar to the ones often applied by large retailers to small, local producers especially in the agri-food chain. And similarly to what happened in retail markets, also for online platforms regulators have gradually found it more convenient to refer to other legislation than antitrust law.

In this respect, several European countries and, traditionally, also the United States (with the Robinson-Patman Act) have legislated to tackle those situations in which, regardless of whether a company is dominant based on antitrust rules, its superior bargaining power or the counterparty's economic dependence create a structural situation of imbalance of power in the commercial relation. Besides general provisions on significant imbalances in commercial relationships, which initially focused mostly on cases of industrial subcontracting, legislators in European Member States have gradually focused also on specific sectors, such as food and retail. In these sectors, often small suppliers are in a situation of economic dependence vis à vis large retailers, and often refrain from suing their large counterparts in case of unfair trading practices (e.g. de-listing, risk-shifting, unfavourable contract renegotiation, etc.), for fear of retaliation (Renda et al. 2014). Over the past three decades, many Member States have tackled this problem, either by stretching antitrust law beyond the rather narrow boundaries of Article 102 TFEU, by relying on unfair competition laws, laws on abuse of economic dependence, rules on the abuse of "relative dominant position" (e.g. in France), contract law, or simply ad hoc legal provisions for the agri-food of the general retail sector (like the UK Grocery Act)[55].

The EU has recently acted to regulate those practices in what is often termed "P2B", or platform-to-business regulation, which 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. In Australia, similar concerns were expressed during the ACCC Digital Platforms Inquiry (see box below).

1.4. Regulating the digital economy: additional, emerging challenges

Apart from the problem outlined in the previous sections, the ever-evolving features of the digital economy are creating new challenges for regulators, which further undermine the stability and fitness-for-purpose of existing regulatory frameworks. This section briefly illustrates some of them: the ongoing "servicification" or "servitisation" of many sectors of the economy, which challenges regulatory frameworks built on product ownership or even "download to own" schemes; the emergence of 3D printing as a form of de- and re- materialization of products; the rise of the "data dividend" as a distributional justice problem in the platform economy; and more generally, the increased use of AI solutions at all layers of the technology stack.

1.4.1. From goods to services: regulatory challenges of the "as a service" economy

The servitisation 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

[55] Laurence Boy, 'Abuse of market power: controlling dominance or protecting competition?', in Hanns Ullrich (ed.), The Evolution of European Competition Law: whose Regulation, which Competition? (Cheltenham and Northampton, MA, Edward Elgar, 2006), p. 220.

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 servitisation 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"[56]. However, the Internet led to an exponential increase in the possibility for servitisation, by allowing what Jeremy Rifkin called, almost two decades ago, the "age of access" (Rifkin 2001). As already observed at section 1.2.2 above, the Internet economy allowed for a virtualization of many functions in the technology stack, drastically reducing the cost of using otherwise very expensive assets such as server computers. Over time, however, the Internet economy has become almost an "everything as a service" economy. Devices are given to mobile customers as a service bundled with subscriptions (and in exchange of customer loyalty); cloud services dominate the market in a large part of the application layer; previously downloaded "to own" software is not accessed online; and even large supercomputers such as GPUs and TPUs are made available on a usage basis through the cloud. Moreover, the "Uberization" of 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" (Prassl 2018).

The main consequence of this trend for regulators is that, generalizing what was observed for the case of the collaborative economy above, most property law, labour law and tort liability rules are being replaced by contractual relations, and thereby by private governance. Importantly, this leads to all imbalances of contractual power to permeate the relationship with no real safeguard offered by the legal system out of contract law. One clear example is the **application of product liability rules for cases in which software is provided as a service**: since the scope of most product liability regimes does not include intangible goods, cases of inadequate services, careless advice, erroneous diagnostics and flawed information are as such thus 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. Moreover, servitization and industry digitalization bring new challenges to the concept of a defect, since various liability and safety issues may arise in relation to automated systems despite the fact that manufacturers and robot designers are focused on perfecting their systems for 100% reliability, thereby making liability a non-issue (Fairgrieve et al., 2013). Similarly, product liability is challenged by the distribution of **algorithmic systems as cloud services**, which, insofar as it appears users receive it as a service rather than as part of a product, would fall out of product liability regimes (AlgoAware 2019).

1.4.1.1 3D printing: from servitisation to re-production

A specific case in the servitisation trend is that of 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. Since individuals become producers of the product, although under third party specifications, it is important that the framework for applying product liability applies to them as well. Without regulatory changes, manufacturers may attempt to evade liability by arguing that they are merely "services providers", renting out 3D printers to clients during the

[56] Hojnik, at 3.

printing process (with the printer remaining at the manufacturer's premises throughout) and selling raw material to clients in advance thereby disclaiming product responsibility.

Additionally, 3D printing turns traditional service providers into manufacturers. Specific regulatory challenges in this respect arise in the medical field where 3D printing enables the printing of replacement body parts, organs, bones and even skin. In this sense, besides providing ordinary patient treatment, medical doctors and dentists provide services, such as constructing a digital design of the implant and printing it in their office on a 3D printer. Low price and high functionality 3D printed medical devices may save lives and have important consequences on social security systems; however, the regulatory framework must contemplate the risks involved and maintain patient safety standards. In the medical devices sector, where 3D printing shows great potential, the classification of 3D printed devices is creating important challenges for regulators: for example, 3D printed medical implants such as prosthetic limbs, hips or teeth are normally classified as "custom-made medical devices" and as such they are not strictly regulated, despite the fact that they potentially pose risks that deserve more stringent regulatory treatment. In 2018, the European Parliament observed that "it will take many years and a good deal of expertise before high-quality products can be made which do not pose a risk to users or consumers. Anticipating problems relating to accident liability or intellectual property infringement will require the adoption of new legislation at EU level or the tailoring of existing laws to the specific case of 3D printing".

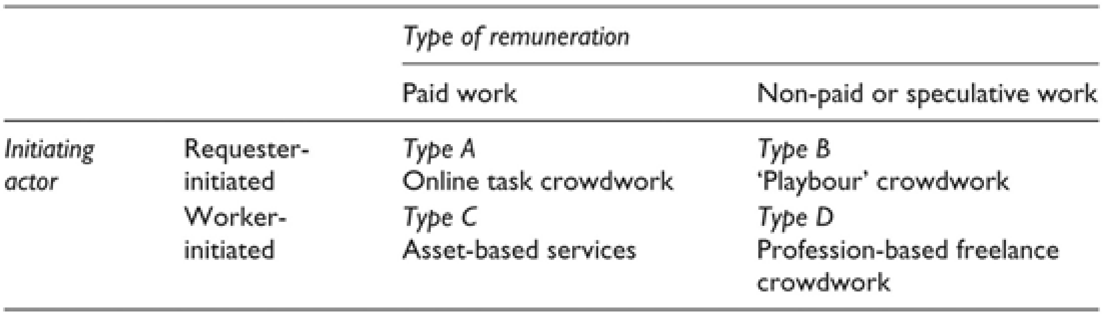
A specific case that is leading to rising concerns among regulators around the world is that of 3D printed weapons. While in most countries any person or business engaging in the sale of a firearm must be licensed, gun laws require that any person buying a firearm must meet certain checks, such as a criminal background or mental health check, before the purchase can be completed, with 3D printed guns these regulatory requirements are almost impossible to verify unless strict control of internet data flows is enabled. In the United States, the regulatory regime currently allows home-printed guns with no specific registration requirements, unless the builder sells or gives away the gun to a third party. The decentralization, digitization and end-to-end nature of the Internet are such that weapons may soon undergo a similar transition to that of songs or movies, which ended up being reproduced with no significant losses in quality, and thereby replicated in a way that leads to almost-complete loss of property; as argued by Thierer and Marcus (2016), the use of Digital Rights Management, already far from successful in the case of p2p file sharing, is likely to be even less suitable to stop uncontrolled 3D printing of firearms. Moreover, while in the case of songs or movies the partial solution was the transition towards a streaming model, in the case of weapons regulatory and public policy concerns become much more urgent and hard to solve: with the foreseen decline in the cost of 3D printing devices over the next 5-10 years, this problem may become so intractable that specific legislation and enhanced controls over traffic data flows may become a compelling choice. The recent lawsuits filed by Defense Distributed to have gun-printing schematics recognized as free speech testify of a constant tension between advocates of permissionless innovation on a neutral Internet and public enforcers; As observed by Thierer and Marcus (2016), "it is extremely difficult and in some cases largely impossible to limit the free flow of information once it has been released on the Internet through peer-to-peer distribution mechanisms and platforms". Likewise, in Australia's New South Wales, a 2015 reform already created a unique offence for possessing digital blueprints for firearms, including a maximum penalty of 14 years imprisonment[57]; but 3D printed guns still occupy a grey area in terms of their legality in many jurisdictions around Australia, as well as many other jurisdictions.

1.4.1.2 When users create free value: challenges of heteromation

As data becomes more and more central to digital business models, regulators increasingly face the challenge of how to incentivize the optimal level of data openness to promote innovation and at the same time protect users' rights. At the same time, the organization of production has witnessed a tremendous shift from labour to capital. Autor et al. (2017a) argue that industries (especially in the digital sphere) are increasingly characterized by a "winner take most" feature where one firm (or a small number of firms) can gain a very large share of the market: possible explanations for the growth of winner take most includes the diffusion of new competitive platforms (e.g. easier price/quality comparisons on the Internet), the proliferation of information-intensive goods that have high fixed and low-marginal costs (e.g., software platforms and online services), or increasing competition due to the rising international integration of product markets. New technologies may also have strengthened network effects and favoured firms that are more adept at adopting and exploiting new modes of production. Autor et al. (2017b) then find support for the thesis that the aggregate share of labour falls as the weight of superstar firms in the economy grows.

The fall in the labour share is also, according to some commentators, due to the fact that many digital business models derive value from the free or low-cost acquisition of key inputs such as crowd-work, or simply data spontaneously posted by end users as in many social networks. This allows for forms of so-called "heteromation", which Ekbia and Nardi (2017) associate with at least five different forms of work that are not fully recognized in the current legal framework: communicative labour, cognitive labour, creative labour, emotional labour, and crowdsourced labour. The latter is broken down by Howcroft and Bergvall-Kåreborn (2019) into four types, as shown in Figure 14 below.

Figure 14. Typology of crowdwork platforms



		Type of remuneration	
		Paid work	Non-paid or speculative work
Initiating actor	Requester-initiated	*Type A* Online task crowdwork	*Type B* 'Playbour' crowdwork
	Worker-initiated	*Type C* Asset-based services	*Type D* Profession-based freelance crowdwork

Source: Howcroft and Bergvall-Kåreborn (2019), Table 1

The same authors report evidence that crowd-working is skyrocketing in many legal systems, with nearly 5 million crowd-workers in the UK, around 12% of the Swedish population is working in the gig economy and 18% of people in the Netherlands have tried to find work via a digital platform already in 2016 (Huws and Joyce, 2016; McKinsey 2016). The most recent World Bank's World Development Report is more cautious on the accuracy of most estimates, and adds with a degree of skepticism that "where data exist, the numbers are still small", and that "the best estimate is that less than 0.5 percent of the active labor force participates in the gig economy globally, with less than

[57] https://www.legislation.nsw.gov.au/bills/5bb4f02b-1f1e-48b2-aa93-955574e699f6

0.3 percent in developing countries". But all depends on the sources and the methodology of research. According to a study conducted by Gallup last year, approximately one-third of the U.S. workforce, about 57 million people, works in the gig economy model[58].

Alongside with crowdwork, more general stances of fair distribution of the value created by large platforms has led to rising calls to recognize the so-called "data dividend", i.e. the contribution provided by end users to the value created by digital platforms. In a recent book, Eric Posner and Glen Weyl advocate treating "data as labour", a situation in which "your personal data, currently hoovered up by tech companies and repurposed for their profit, [are] honored as your dignified work and compensated as such .... "Rather than the growing prowess of digital systems being seen as "Artificial Intelligence" (AI) that would replace our jobs, it would be seen as a new source of well-paying jobs and income supplements. Rather than being treated like passive consumers of the entertainments dished out to us by digital platforms, we would be honored as the suppliers of the data that make the digital economy work. Rather than all the value of the digital economy flowing to wealthy nerds in cosmopolitan cities, the fruits of digital technology would be shared broadly among citizens"[59]. These calls have been recently echoed by regulators in a number of jurisdictions, including most notably California[60]. Commentators have argued that large companies making a significant portion of their profits from data that users create could be subject to a data tax on gross revenues, as a way to restore purchasing power and mitigate rising inequality. This possible future form of taxation echoes calls for slightly different measures, such as "robo-taxes" and Universal Basic Income schemes, which aim at alleviating the inequality impacts of the digital economy.

1.4.2. Algorithms, liability and ethics: towards new policy frameworks

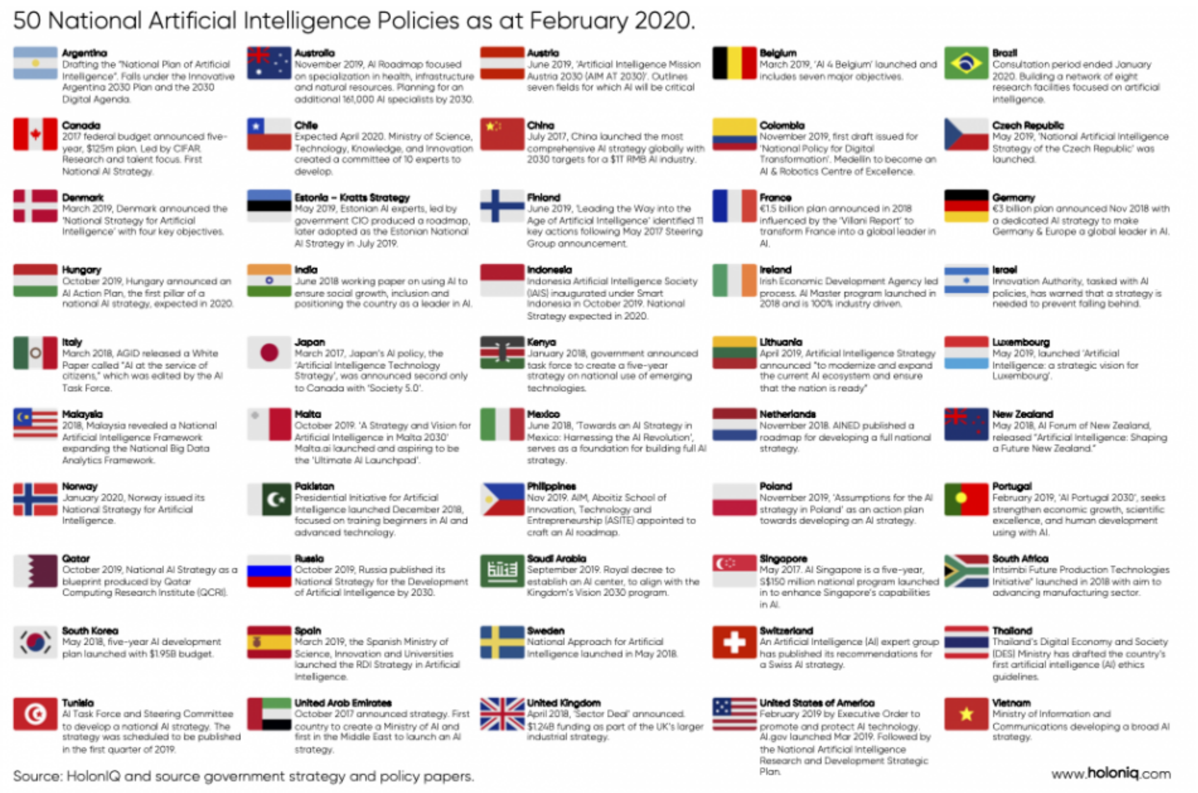
The rise of AI in the digital ecosystem is generating a new set of policy challenges for regulators around the world, which deserve being highlighted since they have brought a plethora of initiatives in many countries around the world. AI developers themselves, and increasingly also corporations and governments around the world have been looking for ways to ensure that the positive disruption and empowerment effects of AI prevail over the potential negative effects. A global dialogue on AI has emerged, which revolves around countless ethical codes and declarations, from the "Asilomar principles" to the "Declaration of Toronto", and the "AI for Good" initiative; corporate ethical principles developed by companies like Google, SAP, IBM, Microsoft, Deutsche Telekom, Telefonica referring to similar terms such as "responsible AI", "Trusted AI", "Trustworthy AI"; guidance for corporate practices developed e.g. by Accenture on tools such as algorithmic impact assessment, or by IBM with its AI Fairness 360 tool; government manifestos such as the Villani report, the Declaration of Montreal, the EU EGE statement and the current draft ethical guidelines on Artificial Intelligence, the Chinese strategy on AI, the UAE strategy, the Indian strategy, etc. (see Figure 15 below); and full-fledged regulatory initiatives such as the EU GDPR, the EU proposed Platform-to-Business regulation, etc.

Figure 15. National AI strategies

[58] https://www.forbes.com/sites/tjmccue/2018/08/31/57-million-u-s-workers-are-part-of-the-gig-economy/#376443d67118.

[59] http://radicalmarkets.com/chapters/data-as-labor/

[60] https://www.gov.ca.gov/2019/02/12/state-of-the-state-address/



50 National Artificial Intelligence Policies as at February 2020.

Argentina
Drafting the "National Plan of Artificial Intelligence". Falls under the Innovative Argentina 2030 Plan and the 2030 Digital Agenda.

Australia
November 2019, AI Roadmap focused on specialization in health, infrastructure and natural resources. Planning for an additional 161,000 AI specialists by 2030.

Austria
June 2019, 'Artificial Intelligence Mission Austria 2030 (AIM AT 2030)'. Outlines seven fields for which AI will be critical

Belgium
March 2019, 'AI 4 Belgium' launched and includes seven major objectives.

Brazil
Consultation period ended January 2020. Building a network of eight research facilities focused on artificial intelligence.

Canada
2017 federal budget announced five-year, $125m plan. Led by CIFAR. Research and talent focus. First National AI Strategy.

Chile
Expected April 2020. Ministry of Science, Technology, Knowledge, and Innovation created a committee of 10 experts to develop.

China
July 2017, China launched the most comprehensive AI strategy globally with 2030 targets for a $1T RMB AI industry.

Colombia
November 2019, first draft issued for 'National Policy for Digital Transformation'. Medellin to become an AI & Robotics Centre of Excellence.

Czech Republic
May 2019, 'National Artificial Intelligence Strategy of the Czech Republic' was launched.

Denmark
March 2019, Denmark announced the 'National Strategy for Artificial Intelligence' with four key objectives.

Estonia – Kratts Strategy
May 2019, Estonian AI experts, led by government CIO produced a roadmap, later adopted as the Estonian National AI Strategy in July 2019.

Finland
June 2019, 'Leading the Way into the Age of Artificial Intelligence' identified 11 key actions following May 2017 Steering Group announcement.

France
€1.5 billion plan announced in 2018 influenced by the 'Villani Report' to transform France into a global leader in AI.

Germany
€3 billion plan announced Nov 2018 with a dedicated AI strategy to make Germany & Europe a global leader in AI.

Hungary
October 2019, Hungary announced an AI Action Plan, the first pillar of a national AI strategy, expected in 2020.

India
June 2018 working paper on using AI to ensure social growth, inclusion and positioning the country as a leader in AI.

Indonesia
Indonesia Artificial Intelligence Society (IAIS) inaugurated under Smart Indonesia in October 2019. National Strategy expected in 2020.

Ireland
Irish Economic Development Agency led process. AI Master program launched in 2018 and is 100% industry driven.

Israel
Innovation Authority, tasked with AI policies, has warned that a strategy is needed to prevent falling behind.

Italy
March 2018, AGID released a White Paper called "AI at the service of citizens," which was edited by the AI Task Force.

Japan
March 2017, Japan's AI policy, the 'Artificial Intelligence Technology Strategy', was announced second only to Canada with 'Society 5.0'.

Kenya
January 2018, government announced task force to create a five-year strategy on national use of emerging technologies.

Lithuania
April 2019, Artificial Intelligence Strategy announced "to modernize and expand the current AI ecosystem and ensure that the nation is ready"

Luxembourg
May 2019, launched 'Artificial Intelligence: a strategic vision for Luxembourg'.

Malaysia
2018, Malaysia revealed a National Artificial Intelligence Framework expanding the National Big Data Analytics Framework.

Malta
October 2019. 'A Strategy and Vision for Artificial Intelligence in Malta 2030' Malta.ai launched and aspiring to be the 'Ultimate AI Launchpad'.

Mexico
June 2018, 'Towards an AI Strategy in Mexico: Harnessing the AI Revolution', serves as a foundation for building full AI strategy.

Netherlands
November 2018. AINED published a roadmap for developing a full national strategy.

New Zealand
May 2018, AI Forum of New Zealand, released "Artificial Intelligence: Shaping a Future New Zealand."

Norway
January 2020, Norway issued its National Strategy for Artificial Intelligence.

Pakistan
Presidential Initiative for Artificial Intelligence launched December 2018, focused on training beginners in AI and advanced technology.

Philippines
Nov 2019. AIM, Aboitiz School of Innovation, Technology and Entrepreneurship (ASITE) appointed to craft an AI roadmap.

Poland
November 2019, 'Assumptions for the AI strategy in Poland' as an action plan towards developing an AI strategy.

Portugal
February 2019, 'AI Portugal 2030', seeks strengthen economic growth, scientific excellence, and human development using with AI.

Qatar
October 2019, National AI Strategy as a blueprint produced by Qatar Computing Research Institute (QCRI).

Russia
October 2019, Russia published its National Strategy for the Development of Artificial Intelligence by 2030.

Saudi Arabia
September 2019. Royal decree to establish an AI center, to align with the Kingdom's Vision 2030 program.

Singapore
May 2017. AI Singapore is a five-year, S$150 million national program launched in to enhance Singapore's capabilities in AI.

South Africa
Intsimbi Future Production Technologies Initiative" launched in 2018 with aim to advancing manufacturing sector.

South Korea
May 2018, five-year AI development plan launched with $1.95B budget.

Spain
March 2019, the Spanish Ministry of Science, Innovation and Universities launched the RDI Strategy in Artificial Intelligence.

Sweden
National Approach for Artificial Intelligence launched in May 2018.

Switzerland
An Artificial Intelligence (AI) expert group has published its recommendations for a Swiss AI strategy.

Thailand
Thailand's Digital Economy and Society (DES) Ministry has drafted the country's first artificial intelligence (AI) ethics guidelines.

Tunisia
AI Task Force and Steering Committee to develop a national AI strategy. The strategy was scheduled to be published in the first quarter of 2019.

United Arab Emirates
October 2017 announced strategy. First country to create a Ministry of AI and first in the Middle East to launch an AI strategy.

United Kingdom
April 2018, 'Sector Deal' announced. $1.24B funding as part of the UK's larger industrial strategy.

United States of America
February 2019 by Executive Order to promote and protect AI technology. AI.gov launched Mar 2019. Followed by the National Artificial Intelligence Research and Development Strategic Plan.

Vietnam
Ministry of Information and Communications developing a broad AI strategy.

Source: HolonIQ and source government strategy and policy papers.

www.holoniq.com

Some of these documents aim at setting global principles or global standards on AI; others at shaping corporate practices to enable compliance with established principles; others at achieving industrial competitiveness, or sustainable development. Many of them also look at how to approach the future policy framework for AI, in fields such as liability, ethical alignment and the protection of fundamental rights. Below, we briefly describe the challenges posed to regulators in these domains.

1.4.2.1 AI and liability

It is important to clarify the rules that apply in case of difficulty to attribute the responsibility to a given AI system. As explained in more detail in Renda (2019), liability issues can emerge due to the following scenarios: (i) a system good causes a given damage, but the individual contribution of AI to the damage is impossible to prove; (ii) an AI system did not incur any malfunctioning, but its interaction with human behaviour led to damage; (iii) an interaction between two or more AI-enabled algorithms has caused damages to third parties (e.g. so-called "flash crashes"); (iv) the combination of two or more AI systems, from different vendors, within a single product leads to damages, with no easy apportionment of liability between the system vendors; (v) it is difficult to prove who, between the AI vendor, the distributor, or the OEM (Original Equipment Manufacturer) has caused the damage.

For example, in the case of the fatal accident occurred in in March 2018 in Tempe, Arizona, when a Uber-operated Volvo car failed to detect a woman that was crossing the street, public authorities took several days and had to closely cooperate with Uber to trace back responsibility for what had happened. Was it the Lidar sensor, and then its producer should be liable? Was it a mechanical failure, and then Volvo should be liable? Was it the camera? Was it Uber, who runs the operating system of those cars? The NTSB Preliminary Report indicated that Uber had deactivated at least two safety-critical features, including emergency braking. But there were also concern that the "human in the loop" was watching a TV show on her phone rather than being ready to step in; but her declarations also raised issues on possible lack of training, which would cause liability to shift back to Uber[61]; moreover, the victim was reportedly under the influence of drugs and alcohol, and it is unclear whether this could have affected the predictability of her behavior, or created issues of contributory negligence (see below). This suggests how burdensome fact-finding can be in complex situations in which several factors cause an accidents[62].

The design of a liability regime for AI inevitably boils down to a fundamental question: can AI be considered as an object under the control of a human being, or does AI feature some elements of autonomy, which would warrant a different set of rules? First, if AI is considered as an extension of the human being, or a part thereof (as could occur in the case of augmented intelligence), then the liability rules applicable to humans will also apply to the AI system. Accordingly, a fault-based regime will most often apply: in many civil law countries, such rule will go back to the Roman *lex aquilia*, which requires a subjective element (negligence, or the intention to cause harm), an unjust damage being caused to another party, and a causal connection between the two.

Second, if AI is considered as equivalent to an object, then the so-called *res ipsa loquitur* (also a common law doctrine) could apply: under this rule, negligence can be presumed if one's property causes harm to a third party. But where no negligence is found on the part of the custodian, owner, or user, liability can be transferred to the manufacturer of the AI-enabled system. This, in turn, will lead to problems of apportionment of liability, as mentioned above, and recently reiterated by Giuffrida et al. (2018)[63]. The alternative approach to *res ipsa loquitur*, as discussed above, would be outright no-fault (strict) liability, which is construed by some scholars also as a fault-based system, configuring a duty to exercise care in monitoring objects under custody (*culpa in vigilando*).

Third, it is reasonable to expect that AI will be used mostly "as a service", especially by SMEs (see Section 2.3.1 above). In that case, it would not be a product but a service that causes damages. In those circumstances, an open question is whether the resulting responsibility for damage caused by an AI system should be of a contractual nature (i.e. provision of a service that does not confirm to sufficient security requirement), which does not exonerate the purchasing party from liability towards damaged parties; or of a non-contractual nature (tort liability), which would then have to be extended to services.

Fourth, an AI system could be considered as similar to an animal, especially when it displays a certain degree of autonomy. This option is possibly backed by authoritative statements in the AI field, which compare the intelligence of most advanced AI systems to that of a small animal, like a frog or a cat. This option would also imply that AI systems have no legal personhood, and that strict liability applies only in case of damages caused by dangerous animals, such as wild animals, if they

[61] The Preliminary Joint Consultation Paper on Automated Vehicles, by the Law Commission of England and Wales, and the Scottish Law Commission, examines the issue of negligence by a "user-in-charge". See https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/11/6.5066_LC_AV-Consultation-Paper-5-November_061118_WEB-1.pdf

[62] Another, less recent example of causative uncertainty is the *Bookout/Schwarz* litigation around unintended acceleration in Toyota vehicles. In that case, the NHTSA struggled to establish the proximate cause of the accident and had to instruct NASA to investigate. After 10 months, NASA failed to form a definitive view about causation.

[63] Giuffrida et al. (2018) also quote the Florida Statute Fla. Stat. § 316.86 (2016) exempting automobile manufacturers from liability when third-party AI is installed: "The original manufacturer of a vehicle converted by a third party into an autonomous vehicle is not liable in, and shall have a defense to and be dismissed from, any legal action brought against the original manufacturer by any person injured due to an alleged vehicle defect caused by the conversion of the vehicle, or by equipment installed by the converter, unless the alleged defect was present in the vehicle as originally manufactured.").

were not duly kept under custody. A similar rule exists both in civil law countries and in the U.S. common law system[64].

Fifth, AI could be considered as a "slave". This interpretation is backed by the fact that the word "robot", in its original Czech word, means "forced labour" or "slave". Soluim (1992) and Hubbard (2011) discuss this option. In Roman law, masters were liable for damages caused by their slaves. And in the United States, a master was liable for every [slave's] trespass, whether the act be done when in the master's service, or not, and whether with or without the master's knowledge.

Sixth, AI could be considered as an employee, and be given legal personhood as well as the duty to exercise due care. Strict liability would still be attributed to their owners, but the AI system would be given legal personhood and could, in principle, be asked to compensate the damage. This perspective appears to be deeply related to the belief that AI systems may display, in the future, a significant degree of autonomy with respect to their "owners" (developers, trainers, programmers, vendors). Recent breakthroughs in AI, mostly due to the use of Deep Learning and Deep Reinforcement Learning techniques, are first steps towards the distancing of the acts of the AI system from the will of the programmer: however, at this stage postulating (like the European Parliament did in 2016) smart autonomous robots with rights and duties seems to be at least premature; and would also lead to a situation in which no certainty is given to damaged parties as to who should, and will, compensate the damage. The same could be said about an even more extreme scenario depicted by the European Parliament: a situation in which AI systems (an in particular, robots) are not considered as employees, but as outright legal persons, with no link to an "owner" or developer.

All in all, the choice between these options should be dictated by a discussion of the reality of AI, rather than its associated myths; by the need to ensure that victims of actions carried out or inspired by AI systems obtain adequate compensation; by the need to avoid stifling innovation by expanding liability to unchartered territories, beyond what is reasonably foreseeable at the time of AI development and commercialisation; and by the need to ensure that humans remain at the centre of both legal rules and AI development.

1.4.2.2 AI and ethics: transparency, bias and discrimination

Guidelines, manifestos, statements, and lists of principles related to AI have proliferated in the past two years. Floridi et al. (2018) compare six of these documents: the Asilomar AI Principles; the Montréal Declaration for Responsible AI; the General Principles offered in the second version of the IEEE "Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems"; the five overarching principles for an AI code developed by the UK House of Lords (2018); the Tenets of the Partnership on AI (2018); and the principles developed at the EU level by the EGE group that advises the European Commission on Ethics of New technologies (2018). Already these documents lead to a total of 47 different principles, although with significant overlaps: if one adds that there are other documents circulating, including i.a. the "Toronto Declaration on protecting the rights to equality and non-discrimination in machine learning systems", the identification of values and principles for AI development already looks like a quagmire. More recently, the AI4People's project has surveyed the aforementioned EGE principles

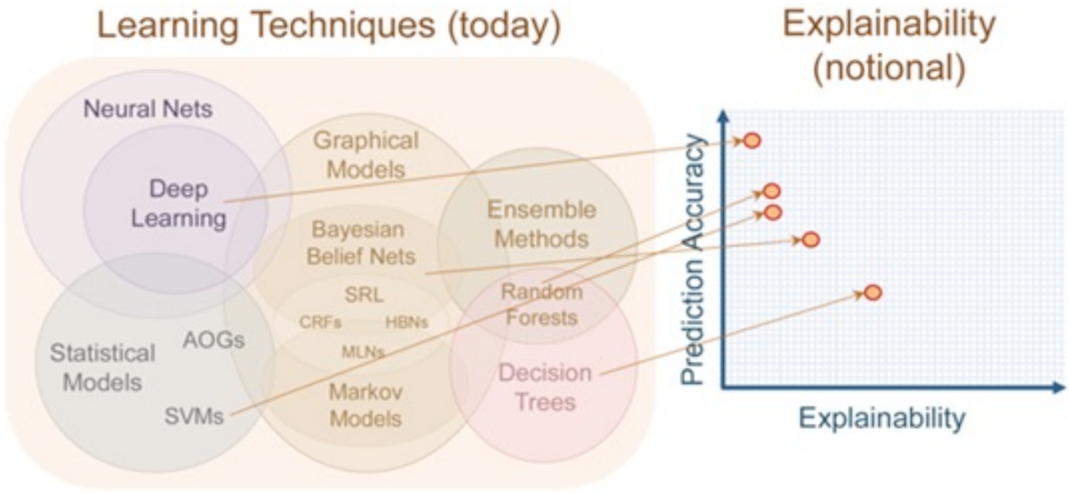
[64] *Behrens v. Bertram Mills Circus*, Ltd. [1957] 2 QB 1, 11 (Eng.). The acts of wild animals give rise to strict liability. Others, especially domestic animals impose tort liability only if harm is foreseeable.

as well as 36 other ethical principles put forward to date and subsumed them under four overarching principles.

The key challenge posed by the need to ensure that AI develops in a way that is ethically aligned is, however, not related to the identification of the key ethical principles, even if the latter already creates some daunting policy concerns (for example, on how to establish a balance, or even a hierarchy between those principles in cases of trade-offs); rather, it is related by the operationalization of those principles in real life. This challenge was recently tackled by the EU High Level Expert Group on AI, which produced Ethics Guidelines that attempt to link principles with an assessment checklist, to be applied by AI designers, developers, distributors and users. Among the key problems to be tackled in this emerging policy space, the following are worth being raised for the purposes of this paper:

On the issue of *transparency*, one of the key problems is the emerging trade-of between algorithmic accuracy and explainability. Figure 16 below shows a sketched analysis of the trade-off companies face between explainability and accuracy of algorithms. In this field, private sector guidance is already advancing rapidly, and is expected to further improve and expand in the near future. For example, Google's Tensorflow recently released a "what-if" tool to visually inspect machine learning models, within the People + AI Research initiative (PAIR)[65]. These systems are able to show the behaviour of the model (as black box) and should gradually move towards a full explanation of how the system reaches decisions, and even more importantly, how the system reached a given decision, for which an end user awaits explanation.

Figure 16. The explainability-accuracy trade-off



Source: Zelros AI through Medium

The issue of algorithmic transparency is even more problematic since it seems to be very specific to the use case. For example, the use of Deep Learning algorithms to handle FOIA requests might violate basic accountability principles rooted in the principles and rules of administrative procedure of most legal systems in OECD countries; the lack of a meaningful explanation in case algorithms reach decisions that impact individual users may lead to an infringement of data privacy rules such as the EU GDPR; and the lack of transparency and explainability of algorithms can have far-

[65] https://pair-code.github.io/what-if-tool

reaching regulatory implications in specific sectors such as education, healthcare, media and news distribution and services of general economic interest, paving the way for uncontrolled discrimination.

The (related) issue of *algorithmic bias* also creates important challenges for regulators, since the option of imposing algorithmic neutrality is not meaningful in most use cases (Renda 2015; 2019). In particular, there is widespread agreement that the use of AI can create unintentional, undesirable bias, thus violating fundamental rights and/or leading to outcomes and impacts that are perceived to be unfair. First, what is undesirable bias? The problem here is that our society is already deeply biased. For example, African-Americans in the United States are much more likely to be pulled off by the police and inspected than Caucasians[66]. Richer people have higher damage awards for personal injury in court, since damages are based on foregone earnings. Women are generally paid less than men in many sectors of the economy, other conditions e.g. level of seniority, experience, evaluations) being equal[67]. Training a machine with data from the real world will in most cases incorporate these societal biases. Not surprisingly, the Google search engine was accused of showing ads for executive jobs more often to what it perceives as white males, compared to African-American women: is this Google's fault, society's fault, or simply a fact of life? As a matter of fact, while biases already exist, the use of algorithms may in some cases exacerbate bias, amplify it, or create it *de novo*. For example, the use of big data and predictive policing techniques in a number of cities around the world has led to concerns surrounding racial biases (Ferguson 2017). In 2016, many commentators argued that "AI is racist", since a beauty contest that was to be decided by an algorithm, supposedly using "objective" factors such as facial symmetry and wrinkles, led to the almost total exclusion of dark-skinned contestants[68]. Similarly problems emerged also in large tech companies, for example when Microsoft released Tay, a chatbot that quickly began using racist language and promoting neo-Nazi views on Twitter; and when Facebook eliminated human editors who had curated "trending" news stories, to discover that the algorithm immediately promoted fake and vulgar stories on news feeds[69]. What makes the issue almost intractable is that there is no such thing as a neutral algorithm: and even if they were entirely possible to achieve, neutral algorithms would in many cases be useless, whereas "excessively" biased algorithms can be dangerous and harmful. Accordingly, it is important to define what biases are to be considered acceptable, and which ones are not. There is also a potential trade-off between accuracy and privacy. In some cases, more accurate algorithms can eliminate bias by avoiding treating people through average calculations. For example, an algorithm may decide not to grant credit to an individual since he or she belongs to an ethnic group that on average repays debts less often[70]. Moreover, the rising use of conversational bots can certainly increase the efficiency of specific services, and even improve user experience in most cases. However, at the same time the risk of discrimination and deteriorating quality of service exists and may be mitigated through

[66] https://www.nationalgeographic.com/magazine/2018/04/the-stop-race-police-traffic

[67] https://www.bloomberg.com/quicktake/why-women-earn-less-than-men

[68] https://www.theguardian.com/technology/2016/sep/08/artificial-intelligence-beauty-contest-doesnt-like-black-people

[69] https://www.theguardian.com/technology/2016/aug/29/facebook-fires-trending-topics-team-algorithm

[70] Using software such as PredPol requires enhanced attention in collecting, curating, using data and avoiding the amplification of bias at all levels of the process . Explaining how bias can creep in while using predictive policing could help clarify the boundaries of their use in police stations, as well as in regulatory agencies (e.g. for data-based inspections). Likewise, explaining how predictive policing can lead to violations of individuals' privacy and how to adopt mitigating strategies would help clarify possible actions to be adopted in all similar cases of use of advanced AI-powered data analytics to predict future events (e.g. the likelihood of a child being abused). See i.a. Virginia Eubanks, Automating Inequality (St. Martin's Press: 2018); and Safiya Umoja Noble, Algorithms of Oppression: How Search Engines Reinforce Racism (New York University Press: 2018).

specific action, including (not limited to) the recognition of a right, for end users, to be informed whenever they are dealing with a non-human interface (so-called counter-CAPTCHA).

Bias and discrimination are also strongly linked to the problem of user privacy, and the related, emerging *trade-off between privacy and security.* For example, the use of personal data from various sources, and in particular from social media, to build and implement a system of social credit scoring is considered as too intrusive and discriminatory based on fundamental rights: however, in many countries data from social media are being used to discriminate between end users, for example in insurance services. The use of facial and/or body recognition, as well as lie detection software can increase the effectiveness of police enforcement. Recent cases have shown that AI can spot criminals among thousands of people, e.g. in a stadium. Advanced image recognition and rendering techniques can also lead to identifying criminals starting from very blurred images. In a time of constant risk of terrorist attacks, massive use of facial recognition is too attractive to be discarded all at once: that said, what are the limits to the use of this technique in the public and private sector? Could a private corporation use the same facial recognition technique used to spot criminals to enable new services in social media, such as matching people with places and advertisers? Could facial recognition be used in combination with other datasets to determine a person's likelihood to repay a debt, and accordingly reach a decision on a user's creditworthiness?

The Expert Group on Artificial Intelligence at the OECD (AIGO) has recently issued scoping principles to foster trust in and adoption of AI, which propose an AI risk-management based approach to enable a balanced set of solutions to the problems outlined above[71]. These principles, alongside with the work ongoing in some OECD member countries such as Canada, Germany, France and the EU, constitute a promising starting point for addressing the substantial challenges posed to regulators by the increased use of AI, in a way that may ultimately help regulators mitigate the risks, while at the same time reap the unprecedented opportunities this technology (and the related ones in the technology stack) create for the global economy and society.

1.5. Delegated enforcement: the challenge of establishing trust between regulators and regulated entities

As already mentioned throughout the paper, one of the consequences of the rise of the digital economy in many fields is a growing distance between the regulators and the act of compliance with the rules, which is increasingly falling in the remit of privatised relationships (as in the collaborative economy), nested in the working of sometimes obscure algorithms (as in the case of AI), or mostly or entirely delegated to code (as in the case of Digital Rights Management and Smart Contracts). This has led regulators to increasingly rely on online intermediaries to enforce legal rules, including i.a. those on hate speech, disinformation, copyright enforcement, antitrust violations and P2B practices. While exploring in-depth the emerging regulatory solutions to the problem of privatised, algorithmic enforcement would fall outside the scope of this paper (which limited to exploring challenges, rather than emerging solutions, see Section 4 below), it is useful to describe some of the key concerns created by this almost inevitable practice in regulation.

First, in cases of legislation dealing with the blocking or filtering of illegal content, the option of algorithmic take-down has raised concerns due to the fact that it would lead online intermediaries to inevitably err on the side of "Type 1 errors" or "false positives" (i.e. in doubt, they take down content even if it is not infringing the law, in order to avoid the risk of incurring liability), thereby

[71] DSTI/CDEP(2019)1

undermining freedom of expression. Such concern was expressed, for example, in the case of the new German Net Enforcement Law, which requires that social media networks check and remove false and hate speech or face a €50 million fine (Echikson 2018). A report by the Swiss Institute of Comparative Law (2017) for the Council of Europe confirmed the concern that "the main issue in this context relates to the consequences of holding the host liable as a co-perpetrator, (at least if) he has knowledge of illegal content", and that "the liability risk to the host might lead to over-removal"[72].

Second, in the case of antitrust remedies related to algorithms, an inevitable concern is related to how is the antitrust enforcer going to verify compliance with imposed remedies, especially since algorithms are often protected by trade secret or other forms of IPRs, and their inspection or auditing is not a widespread solution in most jurisdictions. Given that some of the most diffuse and impactful algorithms are updated several hundreds of times per year, monitoring compliance with antitrust remedies might become extremely difficult, both in cases of abuse of dominance and in those of collusive agreements. Capobianco and Gonzaga (2017), among others, argue for the possible introduction of "auditing mechanisms for algorithms" in the case of possible risks of collusion[73].

Third, in the case of P2B relations, imposing transparency and fairness obligations may impinge on the IPRs related to the algorithms used by online platforms. On the other hand, allowing algorithms (for example, for ranking sellers in a marketplace) to remain obscure to businesses using a platform may lead to discriminatory practices, and even retaliatory ones without any possibility for the law to intervene.

Finally, in the case of fake news or disinformation campaigns several phenomena and possible impacts have to be considered at once when crafting adequate policy remedies. Content bubbles[74]; unintentional fakes/opinions (so-called "misinformation")[75], and intentional fakes or amplifiers ("Disinformation") are very difficult to disentangle without creating risks for freedom of expression. Only in a subset of cases, the lack of filtering on online platforms has led to the abuse of such platforms, with the clear intention to manipulate public opinion, for example in the occasion of an election. Many of these news are ignored by the public as clearly fake, but others spread very quickly and, even if at the margin, affect public opinion creating a thick layer of "noise" between end users and reliable news. The real problem is created by commercially or politically motivated manipulation strategies, a variant of intentional disinformation, but happening at a much greater scale. These operations, which can be state-sponsored, aim at affecting the outcome of elections or at discrediting commercial rivals by purchasing privileged spots for online advertisements and using

[72] SICL (2017), Comparative study on blocking, filtering and take-down of illegal internet content.

[73] https://www.competitionpolicyinternational.com/wp-content/uploads/2017/08/CPI-Capobianco-Gonzaga.pdf

[74] Content bubbles (or echo chambers) are described as a "state of intellectual isolation", which occurs whenever an individual interacts with a single news source, powered by an algorithm that only feeds users based on their perception of what they will like, or be interested in. Described in the past by Nicholas Negroponte and later by Cass Sunstein as "the daily me" problem, this problem is the product of both behavioural biases (such as the "confirmation bias", i.e. we tend to like what we already agree with); and the use of algorithms for personalized search, which are based on our past searches and thus mostly select content from a narrow subset of available sources.

[75] Anyone can express an opinion on the Internet, and share it widely on social networks. Even when one lacks a sufficient number of followers, there are strategies available (or even markets for followers) that can maximise one's own reach in the social network communities. In this context, expressing one opinion, however false (e.g. "the Earth is flat"; "AI will create net employment"; or "trickle-down economics works for the poor"), can fuel disinformation even if there is no underlying intention to engage with manipulation of the public opinion. The Internet amplifies these statements, leading to an unprecedented rate of circulation of both true and false statements.

them to spread intentionally and strategically crafted messages[76]. As appears evident, not all these phenomena should lead to censorship or attempt to block the spread of information. Different opinions always existed, and the diversity of opinions lies at the core of a sound political debate. Different opinions also often reflect different individual preferences, or even different cultural backgrounds. Asking internet intermediaries to filter out non-majoritarian, non-fact-based opinions from the major channels of access to information would dramatically impoverish democracy and society; just like relying exclusively on neutral (relevance- or popularity-based) algorithms for the selection of news feeds would inevitably jeopardise the accessibility of local, niche or anyway "minoritarian" content (Renda 2015). The rise of AI-generated newsletters poses this problem, which requires a careful debate between policymakers and Internet intermediaries. Any policy strategy should think both short- and long-term. In the case of online disinformation, the increasing ability of operations campaigners to spread "deep fakes" and to hide behind obscure and impenetrable IP addresses calls for preparatory actions on the side of regulators[77].

Policy solutions in all these domains are far from easy, and create new challenges for policymakers, which can mostly be summarized in the need to establish trust between the regulator and the regulated. Such trust may take various forms, from the use of algorithmic auditing to the implementation of blockchain solutions for compliance purposes, to the empowerment of end users or third-party certification providers. These possible approaches should be subject to further research and comparative analysis, which as already mentioned falls outside the scope of this paper.

2. EU policy in the digital world: towards a new vision for the Single Market

Over the past few years, the EU has gradually stepped up its efforts in the digital domain, becoming gradually more assertive and determined to address the emerging trends of the digital ecosystem, as portrayed in Section 1 above. It is certainly undisputable, in this respect, that the B2C domain is currently dominated by large US tech giants such as Google, Facebook, Amazon, Apple, Twitter, Microsoft and Netflix, though this dominance is increasingly challenged by Chinese giants such as Alibaba, Baidu, Tencent and Huawei. The two superpowers hardly fight in each other's backyard (at least when it comes to platforms); yet they compete at arms' length in global markets. The US tends to dominate on the software and applications side, but Chinese companies dominate the infrastructure domain, and will increasingly need to serve non-domestic markets once its middle class has consolidated and related markets are saturated. In all this, it is widely acknowledged that Europe has not been (and may not soon be) able to compete on an equal footing with the United States and China in terms of the sheer size of investment in new technologies. A first Communication on AI, adopted in April 2018, acknowledged this investment gap and highlighted a possible alternative strategy for Europe, mostly based on a combination of competitiveness and ethical rules. In other, related fields such as 5G wireless communications, the Internet of Things, online platforms, high-performance computing and

[76] The Russian meddling in U.S. elections occurred exactly in this way: Facebook submitted a written statement to the U.S. congress, revealing that Russian agents created 129 events on the social media network during the 2016 U.S. election campaign: such events were viewed by 338,300 different Facebook accounts, 62,500 of which marked that they would attend. In 2016, campaign advertising on the internet skyrocketed in the U.S., increasing eight-fold since 2012 to an all-time high of $1.4 billion; and is projected to rise to $1.9 billion in the 2018 midterm elections, reaching 22% of all campaign ads. In reviewing its records, Facebook found approximately $100,000 in ad spending from June of 2015 to May of 2017 — associated with roughly 3,000 ads — that was connected to about 470 inauthentic accounts and Pages in violation of its policies; this led Facebook to infer that these accounts and Pages were affiliated with one another and likely operated out of Russia.

[77] In particular, it is clear that the word of journalism will be permeated by artificial intelligence in the years to come. Current trends include i.a.: computational journalism and computer-assisted reporting; i-teams for algorithms and data; natural language generation for reading levels; computational photography; journalism as a service (JaaS), in which rather than reporting solely for their own publications, journalists deliver content that can be used by third parties; real-time fact checking, synthetic datasets and more

blockchain, the Commission has shown similar intentions, but so far relatively poor implementation. In yet another set of high-tech areas, such as genetics and genomics, the EU has remained almost silent despite the fact that the policy debate that emerged over the past few years was ethically loaded.

Could Europe play a leading role in the setting of rules and ethical principles for the development and commercialisation of new technologies? As things stand, the answer cannot be positive. If one looks at the emerging new technology stack portrayed in Figure 10, Europe appears to be lagging behind other regions of the world in many crucial respects: not only the size of investment in R&D&I, but also in terms of fixed and wireless broadband deployment (very high capacity networks, as well as 4G); level of per capita investment in e-communications infrastructure; level of investment in AI, blockchain, the IoT; uptake of new technologies among consumers, as well as among firms; relative development of high-tech skills and competencies; ownership of patents in key enabling technologies; readiness for the quantum supremacy age; and even skills available in the public administration. All this weakens Europe's potential when it comes to credibly proposing (let alone imposing) global standards.

The recent entry into force (in May 2018) of the General Data Protection Regulation is considered by many as a possible exception, which may chart a new course in EU technology policy. By requiring strict standards of data protection, as well as restrictions on profiling, a right to data portability and to receive a meaningful explanation of how algorithms reached sensitive decisions, the GDPR seeks to establish a global standard in the high-tech world, and to chart a new course in technology policy, making it more user-centric after many years of rather drastic laissez-faire vis-à-vis data protection. The GDPR has been implemented only recently, in May 2018, and significant uncertainty still exists as regards its success in terms of improved protection of end users' right to data protection, as well as in terms of actual levels and modes of compliance. Accordingly, it is probably too soon to draw conclusions, yet a few lessons can already be learnt. First, the GDPR has shown that courage pays at the EU level: the decision taken a few years ago on the need for a regulation on data protection has made the GDPR a path-breaking text in a world dominated by relatively lenient data protection rules. Second, Europe has successfully conquered the front pages of the international press, as well as grabbing the attention of top company CEOs through leveraging its ability to draft consistent, comprehensive rules, as well as its large and relatively rich internal market. Third, and relatedly, the EU has discovered that well-conceived, sound technology rules can potentially translate into effective export products, although there is no certainty that this is actually happening with the GDPR.

Assuming that the GDPR will eventually be a success, can the EU replicate this experience in other, related fields? One attempt, as already mentioned, is underway in the field of AI. At the same time, Europe has no consolidated tradition in the ethics of AI, which would help it build credibility in a field in which it has certainly neither research and innovation leadership (with some exceptions), nor a very established infrastructure.

2.1. Preparing for actorness: five reasons why Europe has an opportunity to lead in the domain of digital technologies

Europe can claim to possess five potential opportunities when it comes to setting global standards on emerging technologies. The first is a solid, comprehensive legal framework, which appears more complete and more consistent than the one available in the United States and China. The second is the size of the single market, which remains for now (but not necessarily for long) the richest market in the world: this gives Europe the possibility to dictate conditions to those that want to acquire or preserve market shares in Europe. The third advantage is Europe's potential leadership in the global quest for sustainable development, at a time in which the United States is backtracking from human rights and SDGs, and China is not yet ready to lead. Fourth, rather than a missed opportunity, data policy may become Europe's sharpest tool given the new commitment to creating data spaces, and advance towards sustainable development through the use of data for good. Fifth, while Europe keeps complaining that it does not have tech giants, and that value extraction by online platforms is impoverishing the EU's traditionally strong industrial sectors, technology is coming to the rescue, allowing for new forms of governance that can mirror, more specifically, the EU's traditional way of approaching economic policy.

Awareness of this emerging space is growing in Europe. It is up to EU institutions and member states to leverage these potential advantages, exploit the current opportunity, and avoid being doomed to irrelevance in the coming years.

2.1.1. Europe has the most comprehensive legal framework on digital technologies, but needs to improve it in many respects

No country has the quantity and quality of legal rules on emerging technologies that the EU has. The new e-Communications Code is now following a very comprehensive e-communications framework launched in 2002, and only slightly reviewed over the past sixteen years, while the US 1996 Telecommunications Act was gradually being set aside by piecemeal regulation in the United States. The net neutrality rules in place since 2016 appear stable and balanced, whereas in the United States they are still contested and have been changed very frequently in the past half-decade. Most importantly, the NIS directive, the Cybersecurity Act, the reformed copyright regime, the Audio-visual Media Services Directive, the e-Commerce Directive, the GDPR, the e-Privacy directive and new Platforms–to-regulation and now the forthcoming Data Act, Digital Services Act and New Competition Tool are paving the way for a very comprehensive framework, in which the new technology stack could find a high level of regulatory quality and certainty. In addition to existing rules, interpretive communications and soft law may be needed to promote legal certainty in domains such as AI (e.g. the products liability directive, the machinery directive may have to be clarified or even adapted). Beyond being very comprehensive, the framework is also very protective of users' rights: the GDPR, in particular, appears as a lone bright spot in a world dominated by aggressive use of personally identifiable information for marketing purposes. Yet, the new President of the European Commission Ursula von der Leyen has announced ambitious regulatory measures in this area, expected by the first quarter of 2021.

Of course, Europe's legal framework needs significant reform and updates. In a recent publication, I called for "AI fitness checks" aimed at bringing the EU *acquis* up to speed with new technological developments (Renda, 2019), a proposal that was later echoed by the EU High Level Expert Group on AI (AI HLEG, 2019b). More generally, the legal framework for investment in infrastructure should be reformed to allow for more flexibility at the national level, against specific targets in terms of connectivity, as well as penetration of both fixed and wireless (5G) networks; and spectrum policy should be far more coordinated, and centralised when it comes to the key frequencies needed for 5G.

Most importantly, Europe should make sure that a suitable, consistent framework for data-driven innovation emerges throughout the continent, in order to facilitate data-hungry solutions such as those involving machine learning. This is a daunting task, given the need to strike a good balance between the free flow of data, the need to ensure national security (which is already an exception to the free flow of data), and the need to protect user privacy. The EU can strike a suitable balance by: adopting a full-fledged open data policy, which extends to publicly funded research as well as data held by public administrations; investing in, and endorsing, AI systems that do not make use of profiling based on personally identifiable data; and funding research and innovation projects on the condition that they include the use of privacy-by-design solutions; and establishing legal certainty on ethical rules for AI, including, *inter alia*, the transparency, explainability, accountability and liability of AI systems, so that developers will act in a less uncertain space. Moreover, at the sectoral level, the launch of 'industrial data spaces' announced in the Communication on a Data Strategy for Europe will promote the sharing of data between competitors and new entrants, at the same time ensuring a more competitive environment by avoiding the accumulation of large datasets in the hands of a few large market players. Finally, and more generally, EU policy at the sectoral level should prioritise two aspects:

ownership of data by players that create value by producing goods and services along the supply chain (e.g. farmers); and control of personally identifiable data by the end users.

2.1.2. Europe is still the richest market in the world

Europe is still the largest, richest single market in the world, although its leadership is increasingly under attack by the US and even more so by China. Europe's primacy as a market also means a lot in terms of policymaking: non-EU companies have a strong interest in serving Europe's half-billion consumers, and will accordingly try to adapt to whatever (reasonable) regulatory constraints policymakers introduce in order to ensure that digital technology conforms to the highest standards of user protection, respect for core EU values and fundamental rights. Not surprisingly, the GDPR was well received by many international players, and many of the largest digital companies are complying with it, regardless of whether they are headquartered inside or outside the EU. The GDPR has reportedly already exerted a significant impact on multinational organisations: if anything, the problem is compliance by smaller companies, who are disproportionately affected by some of its provisions. Some companies who may have initially viewed the regulations as a hindrance to the way they can communicate with their audience, will have now realised that the GDPR forced them to think more carefully about how to reduce the amount of data that is being transferred, or how to secure data in case of a cyber-attack or a major disruption of their servers or networks.

There are many ways in which the EU can leverage the attractiveness of its single market. Setting relatively strict rules is not going to be sufficient, if such rules are not fully enforced, and if they are not also applied to non-EU players that want to interact with European consumers. For example, in the case of the GDPR, the extent and mode of compliance with the rules introduced in May 2018 will determine whether, and to what extent, the legislation will have been a success: the first communication on the review of GDPR, adopted in June 2020, concluded that businesses are developing a compliance culture and increasingly use strong data protection as a competitive advantage, but also hinted at a far from satisfactory level of compliance, especially when enforcement depends on cooperation with non-EU authorities. The Commission has thus announced that it will seek authorisation from the Council to open negotiations for the conclusion of mutual assistance and enforcement cooperation agreements with relevant third countries. In other fields, similar problems may arise for future ethical rules on AI: specifying that AI has to be transparent and non-discriminatory may be only a nice gesture, if no procedure is put in place to enforce these principles in a way that is compatible with the features of modern digital technologies: algorithms are constantly changed and updated, and simply requiring specific algorithmic features in legislation may not be easy, due to problems in verifying compliance. A new regulatory initiative is now in the making, but its contours at the time of writing are still rather obscure.

A possible and necessary improvement in current EU policymaking includes the transition towards principles-based, experimental legislation that adopts both *ex ante* and *ex post* technological means of enforcement. The principles-based nature of legislation ensures that as technology changes, market players and citizens are aware that the same set of overall principles and values are embedded in legislation, and that they are invariable to technological change. In the case of AI, as recently advocated by Renda (2019), this core set of rules should include EU core values and fundamental rights, principles of responsible AI generally accepted in the community of AI developers, as well as additional principles that will determine the EU's specific approach to AI, which should include elements of complementarity between man and machine, responsibility in AI development, as well as sustainability.

The experimental nature of EU legislation is essential in order to ensure that innovative services and business models have a chance to be tested before being admitted to the market, and that legislation is stringent enough to steer innovation, but flexible enough to allow new business models to enter the market and improve societal welfare. The use of techniques such as RCTs, real and virtual sandboxes, ideation sprints, regulation through browser extensions and third-party algorithmic auditing can help Europe strike the right balance between the precautionary principle and the innovation principle.

Enforcement should also change: in data-rich digital environments, enforcement methods need to combine both *ex ante* and *ex post* techniques. *Ex ante* techniques include the obligation to leave audit trails in developing technologies, for future consultation by agencies and courts; the adoption of 'privacy by design' and 'fairness by design' tools and standards in the development of AI systems; the adoption of blockchain-based solutions to ensure decentralised control of compliance with legislation; and more. *Ex post* enforcement techniques increasingly require the use of bots to patrol internet traffic, the *ex post* auditing of algorithms, the imposition of strict liability rules and even compensation funds to ensure redress for users damaged by AI systems; and more.

Most importantly, securing the single market through stringent, flexible and well-enforced legislation is only a first step towards leveraging the power of Europe's 500 million consumers. In a world in which large superpowers are likely to adopt less stringent rules than the European ones, Europe will need additional tools to promote its laws and ensure that no 'race to the bottom' occurs in high-tech markets. These may include the use of certification (an 'EU seal' for high-tech products and services); the restriction to EU-certified products in public procurement; the introduction of specific safeguards in the use of high-tech products and services in trade agreements; and more. Only in this way, through a consistent set of rules and means to enforce them, can Europe aspire to becoming a global norm leader, offering market players a consistent, comprehensive environment in which new technologies are promoted, and users are adequately protected.

2.1.3. Filling the empty throne: Europe as a leader in socially and environmentally sustainable technology

It is often said, in the debate on new digital technologies and in particular on AI, that Europe lacks a 'vision' for the medium term. This, however, is not true. Europe already has a vision: Agenda 2030, based on the Sustainable Development Goals. In launching Agenda 2030 back in 2016, and in renewing its commitment in 2019, the European Commission announced its plan to mainstream SDGs (in their European version, most likely more ambitious than the global one) in all aspects of EU policy, including the European Semester, cohesion policy, better regulation, and sectoral legislation. In the negotiations on the future Multiannual Financial Framework for 2021-2027, the EU institutions referred extensively to sustainable development in earmarking funds for specific areas of policy while the new EU research and innovation programme, Horizon Europe, widely refers to the SDGs. The von der Leyen Commission has maintained the SDGs as "North Star" for all Commissioners, for the European Semester as well as for External Action: at the same time, the narrative in Brussels has rather settled on a "SDG mins" approach, well represented by a growth strategy centred on the twin transition (green and digital), and even more specifically by the "Green deal with Just Transition" idea, which is permeating the action of EU institutions.

However, for some reason, when it comes to 'mainstreaming SDGs' in digital technology policy, there seems to be a reluctance on the side of the EU institutions. This may be due to the need to preserve control of specific policy areas in specific parts of the European Commission, without subjecting technology policy to the control of DGs in charge of social and environmental sustainability. But the overall result is very regrettable, for two major reasons. First, Agenda 2030 will be weakened if digital technology policy lacks coherence with overall EU sustainable development strategy. Second, the rules adopted for digital technologies will also be isolated, and ultimately weaker. AI is a perfect example in this respect: asking what rules are best to promote European competitiveness in AI only provides part of the answer; much more important will be to ask how AI can help Europe reach its 2030 goals. The latter include specific goals on decent work, reducing inequality, eradicating poverty and hunger, investing in human capital and eliminating gender bias; and on land use, water, the environment and energy among others. All these goals can be profoundly affected by AI developments, but the link is not being explicitly made, except by the global "AI for good" initiative launched by the United Nations.

Developing a comprehensive policy framework to enable the contribution of digital technologies to the SDG agenda would ideally place the EU as global leader both in the SDG arena, as well as in the technological one. Other global powers have fewer incentives to go down this road, and are currently either in a state of denial with respect to SDGs (US) or in a conflicted position that prevents them from adopting economically, socially and environmentally responsible rules (China).

2.1.4. The data train has not (yet) left the station

Too often EU policymakers complain that European companies cannot compete since data are firmly in the hands of a few large tech companies, mostly based outside Europe. And indeed, current figures show that the bulk of Western world data is currently stored in the United States, whereas a tiny fraction is currently stored in Europe. If data, as many commentators say, were really the 'new oil', then there would be no possibility for Europe to compete on an equal footing with other superpowers. China is rising to the challenge by imposing data localisation requirements on all players that deal with Chinese consumers. In a nutshell, everyone wants data, and if possible on their territory, and there is a growing belief that restrictions to data flows, including the ones introduced by the GDPR for the purposes of data protection, may hamper the development of digital technology, and the competitiveness of legal systems that dare to go down the road of strong privacy and data security standards.

However, this is only a very static way of portraying reality. This is what has happened to date, but there is no reason to believe that it should happen in the same way, and to the same extent, in the future. In a word: the data train is still on the platform and has not left the station. Here's why.

First, in the B2C domain large online platforms have accumulated personal and non-personal data for several years, often without having to pay, and will most likely continue to do so on account of positive network effects, which tend to sustain and reinforce their position in the market. But to the extent that these data will be needed for services of general interest, or whenever these data will be found to represent a significant barrier to entry, public authorities will have the option of requiring access to specific datasets, or even imposing mandatory interoperability requirements on large technology giants. This would be a re-proposition of the essential facilities doctrine in a new fashion, with a specific approach that dates back more than two decades in EU competition law, to cases like *Magill*, *IMS Health*, and *Microsoft* (Renda, 2010). 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. These opinions have also motivated the European Commission to table a proposal for *ex ante* regulatory remedies as part of the Digital Services Act, and even a proposed "new competition tool", which would be based either on the traditional notion of dominance, or on the specific market structure observed, enabling the introduction of remedies even without the finding of an abuse.[78]

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 of the Digital Transformation on EU Labour Markets.[79] 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 a web tax along the lines currently considered by France, which received a first political agreement in the G7 context in July 2019 in Chantilly, France, and which seems to have become even more urgent due to the COVID-19 pandemic. 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. 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.

Third, and most importantly, the current wave of AI-enabled data analytics was spurred by one key factor: the explosion of digital data availability made possible by the first wave of the internet, which connected people across the globe. The availability of an end-to-end digital environment in which ever-growing computing capacity and enhanced broadband connectivity led to the 'zettabyte age', an extremely information-rich environment in which the availability of data in digital form roughly doubles every year: someone, or better something has to process all that information, and the use of AI has become inevitable to accompany this breath-taking development. In 2018, the amount of data created every day had reached 2.5 quintillion bytes, and the data created in the last two years amounts to more than 90% of the data ever created. While this is already mind-boggling, it is also still the beginning, and not necessarily the most important development in the use of data to ensure productivity, growth and prosperity. Given the current evolution of the internet 'of people', it is not surprising to find that the data and AI applications that have been entering the marketplace over the past years, starting from chatbots and recommendation engines to end with AI-enabled cameras for smartphones and personal fitness applications, are often unrelated to emerging existential challenges for our planet such as climate change. The data we need to tackle the climate challenge, and improve our productivity in factories, has not been created yet, and will be massively created in the future thanks to development such as the internet of things, 5G and edge computing. But for these types of data, which most often pertain to the B2B or G2C (government-to-citizens) domains, the there is no obvious leader around the world, and the processing of the information and related AI elaboration (in what is often called 'embedded AI') will take place more locally, and in a less standardised way compared to what happens in mass B2C markets.

In other, simpler words, the race to collect and process data has just started, and Europe has a chance to get it right. While the US and China are increasingly engaging in a digital arms race, the use of digital technologies for sustainable development suffers from a chronic lack of leadership, which only the EU can try to fill. Current initiatives such as the proposed creation of the Global Partnership on Artificial Intelligence, nested in the G7 and backed by the OECD, have initially met the resistance of the US and the

[78] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12416-New-competition-tool.

[79] https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-impact-digital-transformation-eu-labour-markets

silence of EU institutions, and are now slowly taking off. All this is occurring while the data related to climate and biodiversity are increasingly disastrous, and the widespread implementation data-hungry AI/IoT solutions appears as a necessary (albeit not sufficient) condition to bring the planet back towards a sustainable path (See Renda et al., 2019). Rather than complaining about data that are stored in the US, EU institutions could instead grasp that much more data will now be created by connected things, and data can even be created by regulators simply through requiring regulated entities to report data on compliance, in what is often termed 'RegTech', or technology-enabled regulation and public services.

The adequate collection, processing and governance of data in support of Europe's sustainable development strategy, and in compliance with EU data protection standards, is one of the key challenges for Europe in the years to come, The reassuring news is that this future is not written yet, and not compromised yet: but it takes a massive commitment, a significant investment and a certain amount of industrial policy to bring it about in a sustainable way from an economic, social and environmental perspective.

2.1.5. New forms of governance for the single market

One corollary of Europe's 'difference' in digital technologies is that Europe has less to lose from moving from highly concentrated platform-to-consumer (P2C) markets towards more distributed governance forms. In fact, digital technologies today allow for forms of governance that were hardly feasible and cost-effective in the past. For example, the extreme redundancy of decentralised blockchain platforms such as Bitcoin is such that most existing applications have to sacrifice something in terms of speed of synchronisation, or in terms of scalability (Mattila 2020). But increasingly, the world of digital technology is making a broad variety of governance options available to policymakers.

More specifically, the economies of scale that characterise the analogue world are much less present in the digital space. This, in turn, means that markets that previously displayed oligopolistic structures, given the need for large-sized firms that would be able to invest in plants, factories and heavy infrastructure, can now work in a much more agile way. And in many sectors, even tangible assets such as lorries, medical equipment, servers, or drones are now being 'uberised', and require much less investment on the side of market players. If anything, economies of scale have now moved to data. This being the case, adopting interoperability obligations to enable more pluralistic market structures could also lead to configuring the single market in a much more fragmented way: as a common economic space in which public administrations share data between themselves and with businesses (through open APIs); in which citizens have control of their data and choice between a variety of different providers; and in which small competitors can thrive and provide local solutions to local problems, on equal conditions throughout the territory of the Union. This does not imply as such that distributed, or even decentralised forms of governance will always be the most efficient; in some cases, however, despite not being the most efficient, they may prove the most sustainable in the long run, and those less prone to creating inequality and allowing the ongoing distancing between value creation and value extraction in the digital economy.

2.2. New trade-offs and policy paradigms: a tale of three domains

The European Union finds itself in the need to revisit its approach to public policy in online markets; its traditional tendency towards openness and interoperability; as well as its reluctance to engage in industrial policy in the digital environment. The adoption and entry into force of the GDPR represented a first, important step towards a more assertive EU positioning in the digital sphere; and is being followed by many more initiatives at the EU and global level, especially in the fields of AI and in the regulation of digital platforms. This process, still in its infancy, will require a greater ability to engage in technology-enabled regulation and governance over time – in short, the transformation of legal code into software code, i.e. technical specifications applicable to cloud infrastructures (e.g. GAIA-X), the governance of the newly created "data spaces", and even the software specifications of smart contracts. In a nutshell, Lessig's original intuition is finding in Europe a response: from "code, not law" to "law as code", a new era in which policymakers refrain from trying to control technology through traditional law, and rather more to governance of, and by, technology as the dominant paradigm for the future.

2.2.1. The myth of technology neutrality: towards stronger EU industrial policy in the digital domain

Regulating technology *per se* is always seen as problematic, even more when technologies can have both positive and negative effects on society. Similarly, imposing a specific technological design by regulation is also seen as suboptimal by many scholars, given that different business models can best prove their worth in a market context, rather than in the mind of the policymaker. At the EU level, regulation has traditionally evoked the principle of technology neutrality, most notably since the 2002 electronic communications framework. Over the past decade, and particularly since 2009, all spectrum licences in Europe are supposed to be technologically neutral; the same concept is used in the General Data Protection Regulation (GDPR) and in the Directive on security of network and information systems (NIS Directive), both adopted in 2016. In the domain of public services, technology neutrality is a key principle underpinning Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation), the European Interoperability Framework (EIF) and the building blocks on electronic signatures, electronic delivery services and electronic identity under the Connecting Europe Facility (CEF) Regulation.

However, while EU policy can try to be technology-neutral, technology is often not neutral with respect to EU policy. The three domains under analysis confirm this principle. First, some technological architectures are more open than others, and in turn open standards are considered as being more compatible with Europe's quest for openly competitive markets compared to proprietary standards, especially in presence of strong network effects, which lead markets to "tip" in favour of one *de facto* industry standards. Accordingly, as observed by Büthe and Von Ingersleben-Seip (2020), openness in standards and software has become a key priority in EU technology policy over the past decades. This approach was echoed also by the European Commission's approach to competition policy in high-tech markets, for example in the Commission decision to impose mandatory interoperability in *Microsoft*, in which the public policy goal of protecting competition prevailed over the protection of intellectual property (the decision was largely confirmed in 2007 by the Court of First Instance, and never appealed). A similar approach, focused on entry and the sharing of essential assets, was adopted also in the regulatory framework for electronic communications, and survives in new-generation EU policies such as the PSD2.

Second, in the field of AI not all techniques are equally suited to fit European values and policy priorities. In particular, within machine learning a number of approaches such as deep and reinforcement learning display a degree of unpredictability (the so-called "black box" problem), which hardly fits key principles of EU technology policy. These range from transparency to the right to a meaningful explanation under the GDPR. In addition, such techniques also defy the "data minimisation" principle included in the GDPR, and often lead to an undue exacerbation of existing biases. The EU has therefore started to take action to ensure that, especially when AI applications generate significant risk, regulatory requirements apply to impose the development and deployment of "trustworthy" AI solutions, which comply with key principles such as the respect for human autonomy, the prevention of harm, fairness and explainability.

Third, technological evolution gradually enabled the solution of complex problems through less centralised, more distributed architectures. Less centralised architectures promise a number of advantages compared to legacy, primarily cloud-based network solutions, especially from the standpoint of EU policy goals. These advantages include: social sustainability, since more distributed architectures typically entail a more balanced and fair distribution of value and revenues along the value chain; environmental sustainability, especially in the case of edge/cloud architectures as opposed to purely cloud-based ones (Laurer and Renda 2020), but not in the case of completely decentralised an synchronised p2p architectures such as Bitcoin; and competition, especially when distributed governance comes with mandatory interoperability and a plurality of players revolving around common standards. Reliance on decentralised, polycentric governance in technology has a natural appeal to EU policymakers: on the one hand, it enables a less concentrated market structure, and fits well the EU's own polycentric governance (Renda 2020a); on the other hand, it avoids the more anarchic, self-organised nature of completely distributed architectures, as featured by decentralised autonomous organisations. It is no mystery, in this respect, that the European Commission has cherished such as governance model in some of its key digital policies, e.g. eIDAS; has moved to champion "trusted" blockchain applications in new initiatives such as INATBA; and is pursuing a federated cloud model in scaling-up GAIA-X (Renda 2020b).

Despite this background, it would be exaggerated to conclude that the EU has succeeded in consistently shaping its digital policy to reflect its key values and priorities, including competition, fairness, sustainability. Quite to the contrary, during the past two decades EU institutions have been heavily influenced by the apparent success of the "Silicon Valley" model, and often lamented Europe's failure to generate tech giants of the magnitude of Google, Amazon, Facebook, Netflix, or Apple. Even at the time of writing, the need to tech giants in Europe is still a highly debated issue, especially among politicians, often in love with the concept of "European champions". Moreover, the notion of "European values", in and of itself, appears vaguely defined and often instrumentally used. And technological evolution has also gradually unveiled the *naïveté* of Europe's early attempts to pursue openness and neutrality in the digital environment, resulting in a real paradox: the more Europe implemented "open" provisions, the more the Internet became closed and proprietary. This also reflected a lack of adequate understanding of the evolving features of the Internet, a sort of "keys and lamp post" problem that led EU institutions to try to protect the neutrality of the Internet by regulating the relationship between internet service providers (ISPs) and over-the-top (OTT) players, at a time in which the emergence of content delivery networks (CDNs) and, more generally, platformisation, were leading in a totally opposite, and largely unregulated, direction.

Hence the lack of coherence in EU digital policy, which is gradually being addressed by the von der Leyen Commission. Dreaming about Europe's tech giants appears odd, if one considers Europe's emphasis on fairness, trust, sustainability and competition; its focus on data minimisation; its often blunt stance towards the conduct of "superstar firms" and their economic and political power; its "structuralist" approach to competition policy; its emphasis on SMEs and equal opportunities. A coherent EU digital policy would rather celebrate the absence of European tech giants, rather than complain about it. Whether this is what the Von der Leyen Commission will end up doing with the new generation of public policy measures announced in 2020, from data spaces to a cloud federation, remains to be seen.

2.2.2. What are Europe's normative principles and goals?

TRIGGER researchers have analysed the evolution of EU policy and governance in three selected domains: open standards and open source; blockchain and DLTs; and Artificial Intelligence (with a specific focus on machine learning).80 Their analysis reveals a cross-cutting degree of uncertainty as regards the actual goals that the EU is pursuing. A number of tensions are identified below.

2.2.2.1 Competitiveness v. sustainability

Approaching digital policy from an industrial competitiveness viewpoint can end up conflicting with other policy goals more often than is currently mentioned. For example, being competitive in machine learning or blockchain may require disregarding important aspects, such as the energy consumption of mining and data centres. And designing a policy to boost EU competitiveness in AI may conflict with legitimate public policy goals, such as promoting full and decent employment for all in the EU (i.a. part of the Sustainable Development Goal 8). Also from a social sustainability perspective, creating a large market for AI solutions may lead governments and the private sector to use personal data and machine learning systems to develop forms of mass profiling or social credit scoring, which would not be aligned with EU "values" such as the protection of fundamental rights. In this respect, the global competitive pressure coming in particular from the United States and China, hardly focused on sustainability, limits the EU's ability to focus on its policy priorities when crafting and implementing its digital policy.

2.2.2.2 Efficiency v. fairness.

Reliance on digital technologies often promises efficiency increases, thanks to the possibility of solving problems "at scale" and exploiting the potential of greater computing power and very low marginal costs. At the same time, empirical evidence continues to suggest that the collaboration between humans and machines most often reaches levels of accuracy that are greater than the exclusive replacement of human labour with digital equipment. In a recent academic paper, MIT's Daron Acemoglu and Pascual Restrepo identify a possible trade-off between cost-effective AI solutions and the quality of production processes, observing that in certain circumstances the need to cut costs may induce companies to introduce quality-reducing AI systems, at the same time reducing employment opportunities81. This issue becomes even more problematic since when it comes to AI systems, a trilemma is emerging: the most accurate techniques (such as deep learning) are often the least explainable ones, and often the most data-hungry ones, potentially impinging on privacy. Similarly, automated decision-making by public institutions (through use of machine learning algorithms) and private actors (especially via smart contracts) can lead to significant efficiency, but may prove problematic from the standpoint of social justice, fairness and the enforcement of contract law.

[80] See Mattila (2020); Collins and Florin (2020); and Buthe and Von Ingersleben-Seip (2020).

[81] Acemoglu, Daron and Restrepo, Pascual (2019), *The Wrong Kind of AI? Artificial Intelligence and the Future of Labor Demand*. NBER Working Paper No. w25682. Available at SSRN: https://ssrn.com/abstract=3359482

2.2.2.3 Public policy v. private governance

The digital ecosystem has been traditionally dominated by private governance. On the one hand, the Internet per se emerged as an environment in which "code, not law, defines what's possible" (Lessig 1999), and as such public policy has always experience problems in interfering and interacting with the connected digital environment. On the other hand, regulators have decided to adopt a "hands-off" approach to the governance of the Internet since the mid-1990s, both in the US and in Europe, and later around the world. Over the past few years, the rise of "superstar firms" and the debate on "value capture" has led to a recognition of the increased risk for democracy and sustainability created by the digital economy. Policymakers have tried to increase their impact on the digital economy by adopting "traditional" pieces of legislation, such as the EU General Data Protection Regulation, which are still based on ex post enforcement and the role of judges. The low level of compliance observed, and evidence of a still rising power of tech giants, testifies of the limited impact these rules had on the Internet.

Two competing and parallel phenomena will determine whether the future of the digital economy will continue to be dominated by private governance, or will evolve into a more publicly governed model: the emergence of attempts to enact "law as code", thereby embedding legal rules in future technical specifications (e.g. of data spaces, and of cloud federations); and the private sector's tendency to ring-fence governance by relying on smart contracts, with no jurisdiction and no reference to publicly enforced rules. In this respect, blockchain systems and smart contracts are enabling a new kind of platform environment, in which individuals interact according to principles and boundary conditions which they set for themselves using the platform resources, such as smart contracts, with very limited possibility for public policymakers to interfere.

2.2.2.4 Data governance: open or managed?

The past decades have marked a clear tendency towards the adoption of open architectures, aimed at exploiting network externalities. Platforms and other large technology companies have increasingly relied on openness as a weapon in the "winner-take-all" competition that characterises the digital economy: examples include the semi-open architecture of Microsoft Windows and continue all the way to the different approaches to openness of Apple iOS and Google Android; the open source and open standards ("open APIs") used in most cloud platforms (Azure, Google Cloud, Alibaba cloud); and even the open patent strategy followed by Tesla and Google.82

Once a platform achieves a prominent position in a given market context, maximising the number of applications through openness is an effective way to increase barriers to entry, and compete with other platforms for market share. At the same time, when coupled with network externalities, openness often ends up strengthening the centripetal forces that, on the Internet, lead large portion of the value generated by economic activity to be reaped by the platforms themselves (Mazzucato 2018; UNCTAD 2019). Over time, it has become increasingly clear that unmanaged openness, despite its obvious appeal, often crystallises the status quo of the Internet, consolidating the position of already dominant players. Likewise, at a more macro level, emphasis on openness has led most

[82] Open source software obviously has become intricately linked to digital platforms, in that, for example in Google's case, the entire business model largely revolves around the Android OS. It used to be the case in the mobile phone industry that software was embedded into the device acting as the platform, but nowadays, it is the other way around. Android devices are "embedded" into the Android software. The open software, in a sense, has become the platform, which enables the controlling of the data, and which links back to the AI and blockchain domains in the aforementioned manner.

of the user-generated data to end up in a fistful of hands (i.e. those of the five dominant cloud operators, all non-Europeans).

The real common denominator in this regard are the platform giants: Google, Amazon, Facebook, Apple in the West, and Baidu, Alibaba, and Tencent in the East. For example, because these platform giants control most of the data circulating on the Internet, their capacity to train AI algorithms is already distorting the competition in the markets.83 The same is true with platforms and blockchain. One good example is Facebook's Libra initiative, which appears to hold at least a dual purpose. On the one hand, if Libra were successful, by leveraging the data of their social media platform's userbase, Facebook could form an unprecedented dataset of how the flow of capital links to the flow of digital goods and services, amongst other things. On the other hand, by establishing a "decentralised" blockchain cryptocurrency system Facebook could manage to avoid the antitrust opposition it would undoubtedly face if it just directly tried to establish some kind of a privatized global currency. However, Facebook would still effectively control the supply of Libra, so the end result would be largely the same, but the veil of decentralization could be used as a decoy to circumvent antitrust regulations.

Not surprisingly, EU institutions have gradually come to realise that focusing on openness would not entirely serve the interests of a fully competitive market, let alone Europe's industrial interests. The new EU "strategy for data", adopted in February 2020, 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 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.[84] 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).[85]

[83] For example, when Google is asking its search engine users to identify squares from images that contain traffic lights or traffic signs (CAPTCHA), it is quite obvious that these inputs are being used for the supervised learning of Google's autonomous vehicles. By forcing its platform userbase to provide inputs like this in a completely unrelated sector, Google has what could be called an unfair advantage against autonomous vehicle developers who don't have this capability.

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

[85] 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.

trigger

Trends In Global Governance
and Europe's Role

CEPS Centre for European Policy Studies

Fraunhofer
ISI

spi
Sociedade Portuguesa de Inovação

Innovation for sustainability
isinnova

EPFL

ETLA

European University Institute

Freie Universität Berlin

TUM
Technische Universität München

POLITECNICO
MILANO 1863

ESIDG ევროპული კვლევები
საქართველოს ინოვაციური
განვითარებისთვის

EMEA
EURO-MEDITERRANEAN
ECONOMISTS ASSOCIATION

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.