UNIVERSITÀ DEGLI STUDI DI PADOVA

DEPARTMENT OF POLITICAL SCIENCE, LAW,
AND INTERNATIONAL STUDIES

Master's degree in
European and Global Studies

Internet in the European Union: past, present, and future of digitalization

Supervisor: Prof. Lorenzo Mechi

Candidate: Daniele Duca

Matriculation No.: 1239301

A.Y. 2021/2022

Introduction

The Internet is a tool like no other, that has changed the whole communications sector in just a couple of decades. The change has been so quick and dramatic that in just a few years we completely changed our behaviours and habits, becoming more and more interconnected. All sectors took advantage of the new tools and technologies to improve and develop their fields, not without controversies and discussion: data protection, cybersecurity and online trade are just some of the plethora of Internet related issues that sparked in the last decade, and that required complex regulatory answers and frameworks to be developed from institutions all over the world.

The COVID-19 pandemic has sped up the digitalization process, making it mandatory for institutions to ensure everybody the right tools to keep life going, remotely. Remote workplaces, remote classes and remote beers on the Saturdays became the norm, but not for everybody: the pandemic shed light on the fundamental issues and imbalances of the digital transformation. Many areas lacked infrastructures and high-capacity network availability, and many citizens didn't have the tools and the knowledge to live a digital life from home. Moreover, the Internet to many people does not feel like a safe and reliable place, and the same can be said about digitalization and new technologies in general.

I have spoken to a state worker a couple of months ago, in charge of filling the documentation for the local recycling centre. He asked me for my ID and for the last bill of my waste taxes, that I had to manually hunt for in the archive box that I still keep for instances like these. He filled an endless paper notebook with my personal data and the data from the tax papers, taking quite a long time, so much that a queue quickly developed behind me. During the whole filling up process, the operator lamented the fact that the new credit card style IDs are hard to read, and that tax papers have changed making it harder to locate the necessary data. At that point, I mentioned that those IDs have a NFC chip inside, that enables, with a quick scan, to output all the users' data making identification easy. I also argued that a similar QR code-based solution could have been included with the tax papers, making his job way faster. He quickly dismissed my suggestion, mentioning that Internet cannot be trusted, computers cannot

be trusted either, and that paper will never fail, break, or crash unlike these new solutions.

This answer sparked my curiosity: after hearing about people struggling during the pandemic to cope with the digital world and the digital life, and seeing all the efforts made from the EU and from national governments to improve the situation, it seemed to me like nothing had really changed, and that we quickly moved back to square one. Being myself actively involved in the high-tech business as a writer, I realised I didn't know much about the Internet and particularly about the political discussion that had developed around it in the last few years. How is it regulated? Which are the relevant actors? What is the current political situation and what are the main issues at stake?

This thesis aims at answering these questions, working as a baseline for related research on the topic. Firstly, we will go over the origins of the Internet, to understand why it was created in the first place, and to have an idea, even if general, of how it works in practice. This serves two main purposes: not only it helps put into perspective everything that is being decided, discussed, and proposed at the institutional level, but it also serves as a foundation to better comprehend the nature of the power play among the different relevant actors of the sector, which, as we will see, a key element of the high-tech industry. We will also analyse the current digital economy, to understand its characteristics, how digitalized the EU currently is and the implications these tools have on growth and prosperity.

The European Union has been very active towards digitalization, particularly in the last decade. The world of the Internet does include a number of different sectors, that ranges from communication technologies, e-commerce, trade and services of any kind, and it has been a priority to regulate all the difference aspects of these new platforms and services to ensure that the end-users are treated the same way across all the different Member States. To explore this aspect, the second chapter dives into the current EU regulation related to the Digital Single Market (DSM): since the Internet became a service-oriented space, it has also needed a comprehensive policy package that the EU has delivered during the Juncker administration, that started in 2014. Copyright,

security, VAT, Roaming and the whole digital world has been dissected with the attempt to comply to the needs of the public and to make the Internet a safer, more competitive, and transparent environment.

The third and final chapter goes over the current and future political discussion related to the latest regulations by the EU in terms of digitalization. Having an idea of the regulatory framework and of the actors at stake and their interests, it is possible to evaluate more clearly the common trends that characterize the political discussions which are actively influencing and shaping the latest pieces of regulation in Brussels.

1. Origins of the Internet

The Internet has guaranteed fast and reliable interconnection among actors and infrastructures, enabling strong links all over the world and revolutionizing the computer and communication sector in the process. It's a tool that, like never before, improved broadcasting capabilities, dissemination and worked as a medium for many organizations and states to better connect and communicate[1]. Knowing its origins helps to highlight trends and the role of the different actors: states, organizations, and researchers that played an historical role and that shaped the reality we're currently living in. To know about the origins of these particular actors and their actions through the years helps to better evaluate the decisions that policy makers make today when regulating the Internet, and the future plans for policy regarding the Internet, digitalization and the wide world of related services.

The Internet was first conceptualized by Joseph Licklider, an American psychologist and computer scientist who is seen as one of the very first pioneers of modern Internet connections and networks. His vision and developments regarding a so called "Universal Network", or a "Galactic Network", already in the 1960s, paved the way for further developments in the context of what he described, at the time, like man-machine symbiosis, and already talking about a "Mechanical Extended Man" and "Artificial Intelligence"[2]. His work for the Information Processing Techniques Office (IPTO) of the United States Department of Defence Advanced Research Projects Agency (ARPA) was a consequence of the political context and the decisions of the U.S administration of the time as an answer from US president Dwight Eisenhower to the Soviet's progress regarding space technology, particularly to the quick developments of USSR satellite technology. The idea that satellites could be a steppingstone for worldwide telecommunication was hinted by famous writer Arthur C. Clarke, mainly known for his contribution to the 1968 epic science fiction movie *2001: A Space Odyssey* directed by Stanley Kubrick. In 1945, the English author theorized the possibility for space relays,

[1] Leiner, B. M. (2009). A brief history of the internet. ACM SIGCOMM Computer Communication Review, Volume 39, Issue 5, 22-31.
[2] Licklider, J. (1960). Man-Computer Symbiosis. IRE Transactions on Human Factors in Electronics, Volume HFE-1, 4-11.

or satellites, to remain geostationary over the same point over the Earth's equator and working as a tool for reliable radiocommunication, when combined at the correct distance between one another. This idea was diffused in secret among the members of the British Interplanetary Society, and it was later published in the technical magazine specialized in electronics and Radio Frequency engineering *Wireless World*, in the October of the same year[3].

The USSR took the space leadership in the technological war that strongly characterized the Cold War period, being the first country ever in history to launch an artificial Earth satellite that would fly in an elliptical low orbit (LEO) around the planet, named Sputnik I. The satellite was successfully launched on October 4th, 1957, and was quickly announced as a great success in the USSR, and received with a mixture of fear and excitement by western countries. Particularly, the U.S. media depicted the event as the biggest victory yet in the technological war, seriously undermining the credibility of President Eisenhower and his whole administration[4].

The impact that this breakthrough had towards the U.S. public opinion is well summarized in the following piece of a letter to the New York Herald Tribune, written by economist Bernard Baruch:

> "While we devote our industrial and technological power to producing new model automobiles and more gadgets, the Soviet Union is conquering space. While America grumbles over taxes and cuts the cloak of its defence to the cloth of its budget, Russia is launching intercontinental missiles. Suddenly, rudely, we are awakened to the fact that the Russians have outdistanced us in a race which we thought we were winning. It is Russia, not the United States, who has had the imagination to hitch its wagon to the stars and the skill to reach for the moon and all but grasp it[5]."

This triggered the beforementioned response by the U.S. government that led to the creation of ARPA, to answer the particular concern that if the Soviets were already in such an advanced position in terms of development, the chance that they could strike an attack through space by dropping undetectable bombs from the sky to whatever location in the U.S. became more concrete. The goal of the administration was to create an

[3] Clarke, A. C. (Feb. 1945). V2 for Ionosphere Research. Wireless World, 58.

[4] McQuaid, K. (2007). Sputnik Reconsidered: Image and Reality in the Early Space Age. Canadian Review of American Studies, 371-401.

[5] Crompton, S. W. (2007). Sputnik/Explorer I: The Race to Conquer Space. Chelsea House.

efficient defence agency that could quickly answer to the USSR threat, while working very closely to the government and with all the necessary resources always readily available. The idea was to close the gap by enabling scientists and researchers to work freely, under the strong leadership and direct control of the United States Department of Defence[6].

[6] Hafner, L. (1998). Where Wizards Stay Up Late: The Origins of the Internet. New York: Simon & Schuster.

1.1 ARPA

The history of ARPA, later known as DARPA, in the early stages of development is closely linked to its key mentor: Neil H. McElroy. Appointed Secretary of Defence in 1957, he previously worked in the advertisement department for Procter and Gamble (P&G), and he successfully contributed to laying the foundation of modern brand management with his famous 3-page company memo[7]. As explained by Hafner and Lyon (1998), President Eisenhower struggled to communicate and to understand the new needs of the scientific and technological department of the time, and it was for this reason that he entrusted a skilled communicator such as McElroy to mediate with the scientific committee, institution that, at the time, was directed by James R. Killian Jr, president of the Massachusetts Institute of Technology. Even if the two had very different professional and academic backgrounds, both of them shared a strong belief in science, and particularly in the freedom for scientists, engineers and researchers to pursue their own projects and ideas without being bothered by issues of funding, deadlines or purpose.

In Killian's opinion, in fact, what led to the huge technological advances achieved during World War II was:

> "…the freewheeling methods of outstanding academic scientists and engineers who had always been free of any inhibiting regimentation and organization."

There were many issues with such an open and "far-out" scientific research method, the first one being the difficulties of gaining the right amount of funding: after World War II and with particular emphasis after the Sputnik public opinion decline crisis, the U.S. was plagued by the existence of multiple entities, particularly military organizations such as the Army, the Navy and Air Force, that needed money to keep on the race to the Soviets. This meant that these organizations were constantly fighting for the last dollar to spend in research and development of new technologies related to their field, and that for every project, a huge amount of state agencies would claim their slice of the cake, effectively spreading funding to different fields and research, leading to scares resources overall for projects. The second issue was time: such research takes

[7] McCraw, C. (2018). American Business Since 1920: How It Worked. Hoboken: Blackwell Pub.

time, from the identification of a possible solution to hypothesis, actual experimentation, gathering of the results and implementation of the new technologies.

McElroy pushed towards the creation of a centralized agency that would take care of the whole R&D funding management, by supervising more closely all the undergoing projects and selecting the ones that could actually lead to the best results in the technological race against the Soviets. The new agency would solve two key issues: it would make it harder for military agencies to get hold of the R&D money for selfish reasons that would slow down innovation in a time of need; and it would also work as a temporary agency until the long-term projects of Eisenhower's administration, like the creation of the National Aeronautics and Space Administration (NASA) and the establishment of a Director of Defence Research and Engineering, would be put in place.

McElroy plans met the president's and administration's needs, and, in the first months of 1958, ARPA started working with a budget of $520 million and a $2 billion budget plan. These developments, though, didn't last for long: in fact, the budget of the organization was quickly shrunk to $150 million due to the official creation of NASA that was sped up in the months following the launch of ARPA. The creation of the new ad-hoc organization for space related projects meant that all space matters and related research was quickly shifted to the new entity, making the scope of ARPA much smaller and harder to justify, particular in an historical moment when quick development was much needed.

The first ARPA's director was Roy Johnson, a businessman and manager who notably left his $160,000 job with General Electric to pick up the much less remunerative task of leading the R&D organization. He quickly resigned after failing to keep the budget for satellite and space research in ARPA's hands, leaving the agency with a proposal, written by his team, to re-build ARPA in new terms, with new goals, to keep the organization relevant even after most of its field of research was taken away from it. Particularly, the goal of the proposal was to get back to that "far-out" research structure with no questions asked that Killian and McElroy strongly vouched for: a way of operating that that, during the short-lived Johnson era, was not really an option due to

the strict requests and monitoring that the Pentagon imposed on the researchers of ARPA.

Johnson's proposal was taken at heart by the scientific community of the time, that as a whole saw the vacancy of this agency as a big opportunity to get funding and push all the research that had been stalling for years in universities, research centres and companies by lack of funding.

The landscape quickly changed in 1961, Jack P. Ruina took the directorship of ARPA. Being a passionate scientist and a supporter of the idea of free research, he pushed the agency towards the new direction, the one that would eventually lead to the creation of modern Internet infrastructures. His methods, in fact, gave all the necessary tools for scientists to pursue their wildest ideas, while ensuring a rich enough budget to backup this research, that Ruina was able to raise to $250 million after the initial $150 million cap. From this moment onwards, the agency funded many U.S. university research laboratories and worked in close relationship with important institutes, such as Harvard University, MIT, Stanford University, UCB, UCLA, UCSB and many others, as well as some private organizations that ran their own laboratories and research. The peculiar thing about ARPA at the time was that, for the sake of achieving great discoveries that would help in the technological war against the Soviets, it adopted a high-risk, high-reward method, sometimes using research that hadn't even undergone the peer-review process. The strategy quickly paid off, with several projects related to state defence being successfully carried out by the agency.

The work of Licklider, who joined ARPA as the first head of the computer research programme in the October of 1962, started taking into consideration the idea of a networking-based theory, that could lead to deep communication among computers. His ideas were quickly picked up by his successors at ARPA, Bob Taylor and Ivan Sutherland, along with several MIT researchers such as G. Roberts and Leonard Kleinrock. Particularly the latter, had published the very first 35-page paper regarding packet switching theory in 1961, and went on to publish the first book about

communication nets[8]. We'll expand on packet-switching later, but it's the core technology that made the Internet as we know it today possible, making the idea of networks realistic.

It was in fact Kleinrock that convinced Roberts that it was theoretically possible to make units communicate using packets rather than regular circuits. This led to extensive research and attempts, that went ahead to create the very first connection between two computers, the Q-32 in California, and the TX-2 computer in Massachusetts. This was a time when computing research in general was stalling, due to the lack of cooperation among the different universities, laboratories, and people, each following similar projects going on their own separate directions, without cooperation or information sharing. That is why the experiment was met with criticism from some actors inside the agency. Nonetheless, the experiment went on, thanks to ARPA's officials supporting the project, under the request that Tom Marill carried out the experiment under the sponsorship of Lincoln Laboratory officials, where TX-2 was located. Using a special Western Union four-wire full-duplex service, that guarantees simultaneous transmission in both directions between two points, like land-line telephone networks do, Roberts along with Thomas Marill, were able to make two computers communicate with each other, using network packets. This is known as the first actual network experiment, and made the researchers realise that it was in fact possible to make computers work together, running programs, sharing, and retrieving data, even if they quickly realized that to do so, the circuit switched telephone system was completely inadequate for the job. New technologies were needed to allow for the creation of a wide-area packet-switched network.

One of key takeaways from this historical description of ARPA is that, even if the Internet was born exclusively thanks to the agency and the funding by the state towards the Department of Defence of the U.S., the progress in computer science research and innovation was achieved by scientists working for the sake of science and technological development. Ideas and research always started from laboratories and research centres,

[8] Kleinrock, L. (1964). Communication Nets: Stochastic Message Flow and Delay. New York: Mcgraw-Hill.

and this is a key concept that needs to be stressed when discussing about development and security: policy makers attention must be targeted towards these people first, to ensure a deep understanding of all the matters at stake when discussing Internet and telecommunication development.

Before going ahead with the description of ARPANET, a more technical explanation, even if simplified because of the nature of this writing, of the difference between packet switching and circuit switching is required, in order to understand the need for new infrastructures related to networking, as opposed to the regular telephone lines infrastructures that were already in place and well known at the time.

Circuit-Switched Networks

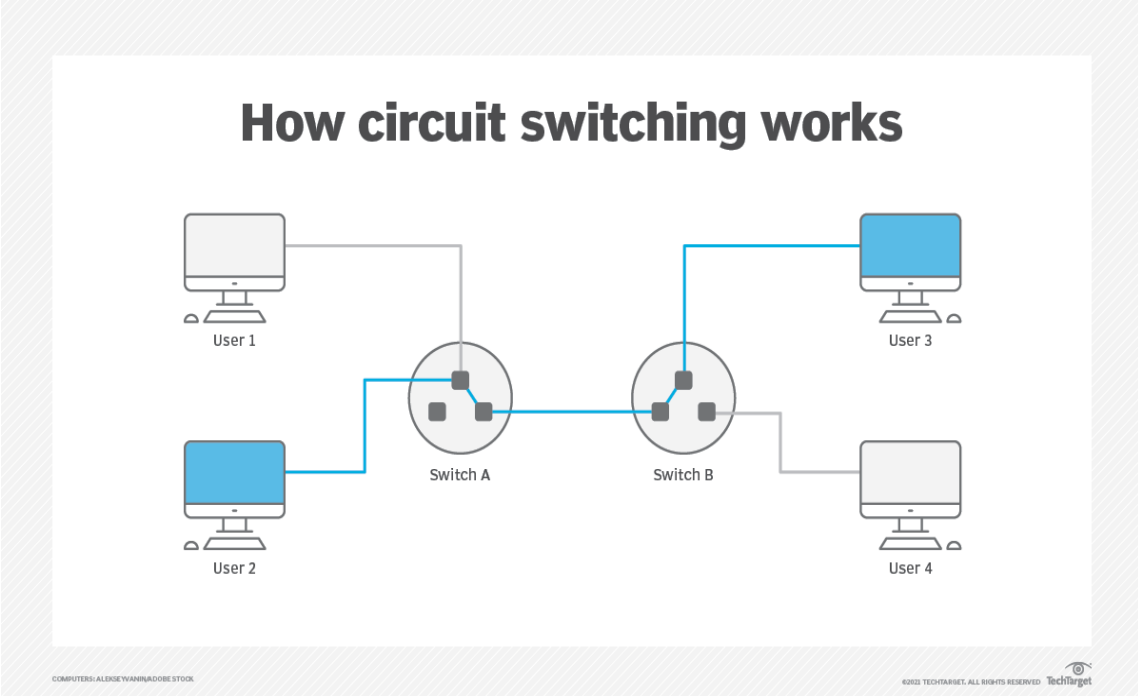

Figure 1. How circuit switching works. Source: techtarget.com

In circuit-switched networks, a dedicated channel or circuit is established for the duration of communications between two network nodes, working as if the nodes are connected with an electrical circuit. This is the technology used by regular phone services, but it has been also used for connecting to the Internet in later days, using dial-up network connections.

The connection and relative infrastructure were built between the end of the 19th and the beginning of the 20th century, the process being started by the Bell Company in the U.S.[9]: as a result and following the great liberalization of the whole sector, the backbone of the phonelines is privately owned.

Being impossible to connect all lines among each other simultaneously due to the 1 on 1 nature of the connection, this technology gave birth to a new profession, the switchboard operator, that would manually connect the right cables to link the two ends of a call.

Optical circuit switching, a variant of this same technology, has been used to meet the growing bandwidth requirements and to scale data centres in more recent years, but at the time it was unthinkable to apply this type of technology the create an open network that would connect various computers among each other, as opposed to just two[10].

[9] Metcalfe, R. M. (December 1973). Packet communication. Cambridge: MIT.

[10] Raja, A. L. (2021). Ultrafast optical circuit switching for data centres using integrated soliton microcombs. Nature.

Packet-Switched Networks

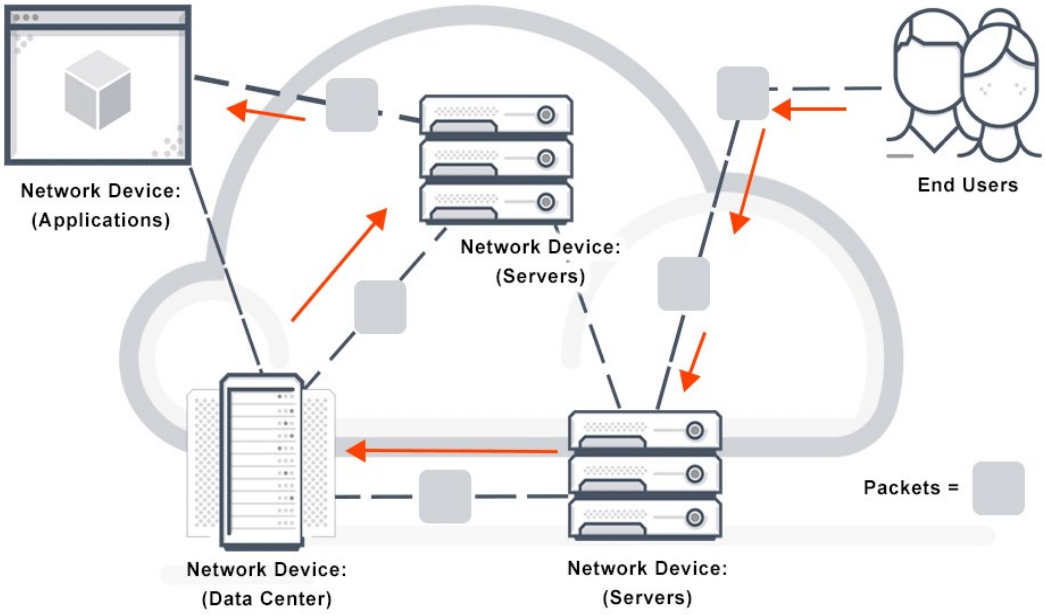

Figure 2. How Packet Switched networks work. Source: avinetworks.com

The breakthrough of telecommunications that eventually led to the development of the Internet like we know it today was a new type of computer communication network, that could send data in groups, in the form of small packets, towards different paths at different times[11]. By taking up the whole line until the connection is set off, circuit switched networks effectively took up all available bandwidth every time a connection was established. This was an ineffective way of sending data, particularly in later times when more bandwidth was needed to offer more and more services to customers. This meant that it became more cost-effective to rebuild and redesign communication networks, introducing packet switched networks that allowed for a dynamic allocation of data bandwidth, granting more users to access the same transmission line.

Even if it appears to be a merely technical concept, it is clear that economic interests also played a huge role in creating a different, more capable type of network: with packed switching more users could connect to the network, making the service more

[11] Roberts, L. G. (Nov. 1978). The evolution of packet switching. Proceedings of the IEEE, 1307-1313.

scalable and adaptable. Moreover, already a few years after this technology was adopted worldwide, routers became cheaper than lines, making it way easier to send gateways to users and keeping the expensive lines as they were. Tech companies, particularly in recent years, due to the high demand of services, invested heavily on new undersea optical fiber cables, capable of high data bandwidths. Nowadays, all telecommunication infrastructure and backbone is built to satisfy the needs of the digital communication, the Internet and all related services, meaning that the whole system is in the hands of the private sector.

1.2 ARPANET

ARPA went on to pursue the idea of connecting multiple computers to quickly share information among researchers, following the lead of the numerous scientists that partnered with the agency and that required better communication tools to share their work. This could eventually work not only as a tool for better research and communication but could also aid in the Cold War against the Soviets: in fact, as we already mentioned before, one of the worries of the American administration was the possibility of a nuclear missile attack from overseas or a sudden and unprecedented sky attack. The idea that it could be possible to build widespread computer control rooms connected to the same network, able to quickly and automatically send an emergency message, particularly in cases were one or more computers, or nodes, got removed from the network, was the perfect plan for the U.S. needs at the time, and could also lead to the creation of an international network defence system for all NATO countries.

In 1968, ARPA sent out a quotation and eventually selected Bolt, Beranek and Newman Inc. (BBN) to serve as master contractor for the creation of the network. The collaboration with BBN led to the use of Interface Message Processors (IMP) to connect the computers and get them to speak the same language, allowing for simple but effective communication. These devices can be thought as the Internet routers of today, functioning as gateways interconnecting local resources: the IMP was connected to the host computer, enabling the very first packet-switched connection among computers to be possible.

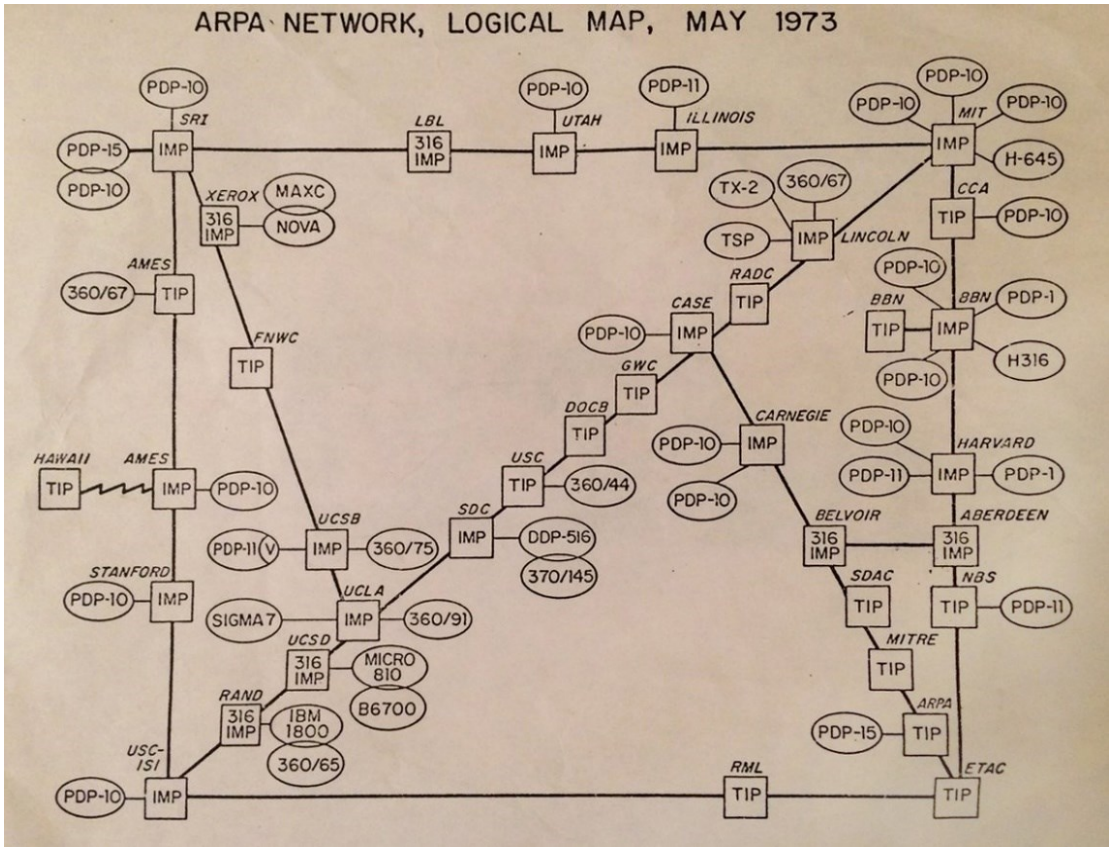

Figure 3. Logical Map of the ARPA network in May 1973.

The first IMP was delivered to Kleinrock at UCLA, and then, a month later, a second device was put in action in SRI. Using a pre-existing network line to connect the 2 IMPs, on October 29th, 1969, Charley Kline in SRI decided to try to log on to the PDP computer in Stanford University. In order to do this, it had to be typed on the local machine the characters "LOG" to which the remote machine would type in "IN". Unfortunately, the remote system crashed during the process, making that "LO" was the first ever message sent over the Internet.

In the months and years following this historical moment, the University of Utah and the University of California, Santa Barbara were added to the network receiving their own IMP's. This was followed by the very first overseas connection to the University of London. Because it was on the other side of the ocean and thus couldn't be connected via the typical phoneline that was used for all the other systems in the U.S., this node was the first connected through SATNET technology, a satellite-based communication system (Hafner, 1998).

The thing to note is that the Internet as we know it today includes al various sorts of connections, and the London case was only the first instance of a process that eventually led to an open architecture, that quickly transitioned to a widespread infrastructure: this coincided with the private sector starting to heavily invest on the quickly growing sector, realizing that it had a lot of potential particularly in terms of services. The first, big instance of a "service" provided through the Internet is certainly the case of the email. This tool was first born during the late 70's, thanks to the contribution of Ray Tomlison, who created a system able to send messages among different hosts connected to the ARPANET system with ease.

After 1973 progress was very rapid, and this meant that other packet-switching networks, independent from ARPANET, started to be put in place in various parts of the world, with other companies producing their own IMP's and starting to sell services to customers. Researchers of all countries and corporations started communicating using their own networks for specific types of collaborations and activities. Already in the 1970's, companies started selling access to specific networks, thanks to the shrank in size and price, and following raise in popularity of consumer home computers. These networks gave access to the very first services, other than being just a tool used to communicate: this moment creates the line where the modern view of the Internet, made of a layer of services of any kind, started to become the most lucrative and interesting part for companies, of the whole technology.

One of the first notable instances of this was CompuServe's MicroNET, later renamed CompuServe Information Service (CIS), a network that using dial-up technology, gave users through the 70's and the 80's the chance to access updated weather reports, emails, the first online games and chatting using the first ever instances of instant messaging programmes. Thanks to an agreement with some of the major newspapers, users could even access the latest copy of The New York Times, The Washington Post, San Francisco Examiner and many others.

At this point, the growth became faster than ever: for instance, from 1985 to December 1994, the Internet grew from 200 networks to over 45.000, which translates

in less than 1000 end-users, or hosts, to more than 4 million. These users at the time were mostly educational sites, commercial sites, and military sites, with just a fraction of these being out of the United States and users being still a low number compared to today, even if cheaper computers and connection costs thanks to the great liberalization of the 90's, quickly created the open network that we are used to connect to everyday[12].

This growth coincided with the adoption of the World Wide Web as a standard to Internet navigation. The platform that enables everybody to connect and to research everything at any time, was invented by Tim Berners-Lee, a British researcher at the European Organization for Nuclear Research (CERN) in 1989, when he submitted a paper that shared the first ideas for Hyper Text Markup Language (HTML), the language still used today as a building block to the web, even if in a more refined and updated form[13]. August 6th, 1991, is commonly referred as the birthdate of the World Wide Web, date that coincided with the publication of the very first website. Thanks to a piece of software, the one we nowadays refer to as a *browser*, Berners-Lee made it possible just 2 years later in 1993, for all users to access the WWW. He made the source code public, enabling everybody to build their own website and consequently expanding the market to a whole new level.

[12] Joseph P. Bailey, L. W. (1995). Internet Economics. Hattiesburg: MIT.

[13] Berners-Lee, T. (March 1989, May 1990). Information Management: A Proposal. CERN.

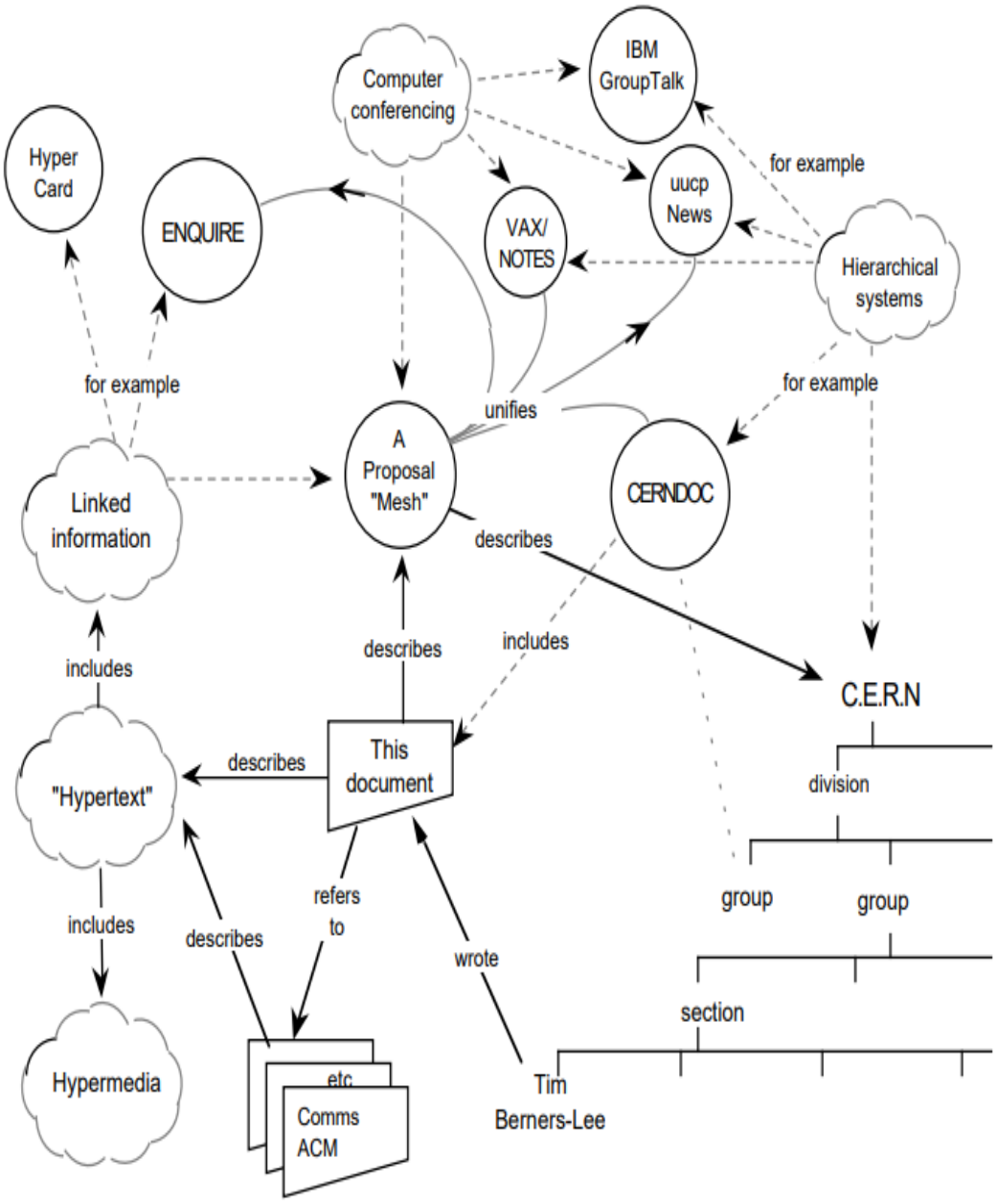

Figure 4. A graphical representation of all the steps, layers and connections required to manage and operate the World Wide Web.

A different story is the one related to mobile telephony and remote Internet access via enabled devices. In 1981, mobile radio telephone systems were firstly introduced to the market, under the name of 1G, with a new mobile generation being developed

approximately every ten years ever since[14], with a strong rise in demand for wireless networks, that is still going on today thanks to the latest technological advancements, mainly 5G.

Going back to 1G, it was based on analogic protocols that would support just a regular phone conversation, with a speed of 2.4 Kbps, and was quickly surpassed and dismissed in favour of its upgraded and refined version. This technology, that was based on digital instead of analogic connections, granted great benefits: thanks to the improvements in bandwidth and general connection quality, SMS became a reality, and the digital nature of this network also led to lower battery consumption, that made easier for mobile phones manufacturers to develop more advanced phones. This was a crucial step, because it heavily pushed the mobile phone market, helping Internet to get in the hands of even more people.

The real change came with 3G, that met the needs of more bandwidth because of the quick raise in popularity of online data services. With speeds up to 2Mbps, a substantial leap from the 64 Kbps offered by older 2G networks, this was the first wireless technology to use packet switching technology, that led to a complete transformation of the industry of telecommunications. Radio, Music streaming and TV streaming on mobile devices was now possible thanks to the first real high speed IP data network.

Today 4G is what most people is connected to, at least in the U.S. and the EU. The increasing demands for bandwidth by audio/video online streaming services kept the innovation flow going, with the development of a new all-IP based network design that eliminated circuit switching completely, providing speeds up to 100Mbps.

But probably the most game braking revolution of recent history is the one that we've been witnessing in the last 2 years with the advent of 5G, that brings some key developments that will dramatically change how companies use mobile networks. The following table makes it clear why the attention has drastically shifted towards this new technology. With speeds up to 10Gbps, latency becomes almost imperceptible, making every operation practically instantaneous.

[14] Pathak, S. (2013). *Evolution in generations of cellular mobile communication.* Bhopal: National Law Institute University, Bhopal

Download times & Streaming	2G	3G	4G	5G
Maximum Download Speed	0.3Mbps	42Mbps	1,000Mbps	10,000Mbps
Latency	500ms (0.5 seconds)	100ms (0.1 seconds)	50ms (0.05 seconds)	1ms (0.001 seconds)
Accessing typical web page	3 minutes	4 seconds	0.5 seconds	near instantaneously
Downloading high-quality photograph	3 minutes	4 seconds	0.5 seconds	near instantaneously
Sending an e-mail without attachments	1 second	<0.1 seconds	<0.1 seconds	near instantaneously
Downloading an music track (MP3)	7 minutes	10 seconds	3 seconds	near instantaneously
Downloading an application	40 minutes	1 minute	8 seconds	near instantaneously

Figure 5. 2G, 3G, 4G and 5G compared, in terms of download speed and overall latency.

We'll discuss more fondly about 5G in later parts of this writing, since it's a topic that is receiving a lot of attention from organizations and policy makers.

What about the use of Internet today? Data from --- shows that 91% of all families in the European Union has access to the Internet, and 86% of people regularly – meaning at least once a week - used online services, with 80% accessing it every day. Even if these numbers seem very high and good for the time being, there is still work to do to get 100% engagement in particular countries, such as Greece and Bulgaria, where one in five people has never connected to the Internet in their entire life[15].

[15] European Commission. (2021). *Digital Economy and Society Index* . Bruxelles: European Commission.

1.3 The travel of data in modern Internet and its layers

Nowadays, the Internet is everywhere, and our life is more connected than ever, all thanks to those scientists and pioneers that worked for the sake of science and innovation, more than for economic interests. But to understand the economy related to it and the following regulation and policies that the European Union employed to try and tame this giant entity, we need to underline all the different mechanics, structures and systems that make it work, even if in a simplified way. A simple web research on the Internet could seem a quick and easy thing to perform, but the layers involved that make up the working structure of the system are many and every single one needs to be accounted for when discussing modern Internet economy, legislation and decision making.

Let's start by understanding what happens when a simple web research is performed by any device connected to the network. Starting from the user side, the Internet is accessed using a web browser, that has been previously installed on a device such as a smartphone, a computer, a console or a web-enabled equipment of any kind. The connection is achieved thanks to an Internet Service Provider, or ISP, which is the organization that provides wired or wireless access to the network by physically building, operating and managing the lines that carry the signal from a location to another. The Internet service provider processes the user's request for connection to a name server, that associates to an Internet Protocol (IP). Every website and user have their own IP address that lets the user and the ISP know how to process the request and which hosts to connect to during a session. When a user wishes to visit, for instance, the website of the European Commission https://ec.europa.eu/, the website promptly responds to the user's request by sending the requested data in the form of packets, which are then formatted to comply to the adequate protocol used to connect the devices to each other and make them communicate. The data then travels to the user's ISP, which ultimately delivers the data back to the user's device of choice, processed and rendered by the same web browser used to perform the request in the first place.

To further understand the structures and the inner workings of the Internet, we need to take a look and the current model in place for interconnection, the OSI model. The

model was conceptualized in 1984 by the ISO, the International Organization for Standardization, an independent, non-governmental organization that ensures Standards for many technologies, with the objective to achieve fairer and better competition in the free-market economies, and to improve product quality, reliability, interoperability, consequently reducing costs.

OSI is a layer-based abstract model of network architecture, built to describe the interoperable standards of computer communication. In other words, it describes how data travels from a computer to a network and then back to another computer, despite the system's internal technology or specific protocol suites. This was done to enable competition in the market and to allow for the technology to easily spread without the growth of different patents and standard that would inevitably undermine the openness of the market. The model is composed by seven abstract layers:

1) The physical layer, that defines the physical characterises of the Internet interfaces, the signals, the cables, the connectors and how the signals actually travel in the infrastructure.
2) The data link layer, where the Ethernet operates, and that enables the connection among hosts on the same network and syncs devices that operate at different speeds.
3) The network layer, the layer where routers operate, enabling host computer connection among different networks and routing the packets towards the right path in the network to ensure that the data reaches the destination. Here lies the IP protocol, and congestion is controlled by routing data to specific paths in the network so that packets don't gather in the same place slowing down the transfer and impacting on the QoS. This layer does not play a role if computers are in the same networks, in that case, the data link layer will operating the connection.
4) The transport layer, where the data is transferred among different computers using connection-oriented or connectionless TCP/UDP protocols. Among other things, such as defining the Quality of Service (QoS) and establishing the end-to-end connection, this is the layer where data is split into smaller packets, that once reached the desire destination get reassembled together.

5) The session layer, that establishes the dialogue among computers inside the network, effectively putting to work all the necessary tools and steps to begin and close a connection.
6) The presentation layer, that establishes how the data is formatted and translated, effectively preparing the data converting it to the right format for the following application layer. This is a very important phase for security, because it is in this particular layer that data encryption and data decryption takes place, along with protocol conversions and data compression and decompression.
7) The application layer, that includes all network applications such as the web itself, e-mails, file transfer etc. This category is the closest to the end-user and does not include applications locally installed on a PC, but only those applications that directly interface to the Internet or that have some type of file sharing or cloud access[16].

The fact that the Internet is so complex and that needs a large number of different actors, levels and tools to be working, makes clear why we can't just think about the Internet as a single case study, but instead that it is required a much wider approach that splits this entity into multiple levels each one with its own regulations, economy, and needs[17].

A quick distinction among the two types of Internet Service Providers and the technologies they employ is also useful in order to render the following chapters more clear: the wirelines ISP's, which use connections such as satellites, DSL, cable modem and fibre. Satellite connection is the oldest and is technically the same one used in the 80's to connect the University of London to the ARPANET, working through a device that communicates with the network sent to and off the satellite. DSL service is an upgrade that the old telecommunication companies employed to their existing infrastructures to start selling Internet services to customers using the existing telephone lines, without being forced to invest in other types of systems like fibre-optics.

[16] Tomsho, G. (2016). Guide to networking essentials. Boston: Course Technology.
[17] Benkler, Y. (2000). From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access. Federak Communication Law Journal 52.

Wireless ISPs operate differently, with the option of a service available anywhere, that helps connecting low-density locations that still lack the wiring necessary to connect to the Internet via wireline[18].

[18] Solum, L. B. (2003). The Layers Principle: Internet Architecture and the Law. Social Science Research Network Electronic Paper Collection.

1.4 Economics and power: the liberalization of the telecom market

Quickly during the history of the Internet, the actors at play shifted from a few Universities and the U.S. government that still viewed the ARPANET as a defence tool in the war against the Soviets, to new telecommunications carriers and particularly old telecom monopolies that already had the backbone put in place, and were able to use those lines to give services to the users even before switching to the traditional high bandwidth infrastructures based on optic fiber that are today's standard.

The first important step, that forever changed the balance and structure of power of the Internet, is the great liberalization, that took place in the telecommunication sector at the end of the 20th century and that greatly revolutionised both the U.S. and the European market.

At the beginning of the 90's, in Europe, telecommunication organizations were owned and managed by local governments, except for the United Kingdom, that operated a privatization of its national telecom firm, admitting partial competition, as early as 1984 and 1985. Some countries followed the example of the U.K., but many others did not allow for a competitive market until the later years of the 1990's. The situation in the European Union was not very welcoming for the new technologies, and the big monopolies played a negative role in the market, which had very high telephone tariffs for customers, with varying costs for local calls depending on the time of the day. This situation hindered the development of the Internet in the early 2000's.

Touching briefly on the regulatory perspective, it was very hard to open the European telecom market to competition and allow for privatizations. The strength of these state-owned companies, and the reluctancy of many states to give up their power over these organisations, was a giant obstacle that slowed down progress for many years, shrinking the pool of customers. Particularly, politicians, as well as companies and stakeholders that had interests in keeping the monopoly as was, used heavy lobbying tools to avoid the EU to implement rules similar to the ones that had been already in place for years on the other side of the ocean.

During the mid to late 90's, the European Union began legislating and regulating towards the liberalization of the telecom market using the common tools used by the EU in these cases, such as papers, directives, and recommendations, with the final stretch being made in 1998 that imposed governments to liberalize and allow for the access of new companies into the telecom market, putting a nail in the coffin of the era of the big monopolies. The Commission ruled in favour of national regulatory authorities (NRAs), that shared part of the legislative responsibilities with the member states and enable them to create new agreements and arrangements to improve competitiveness and allow for more companies to take a share in the now thriving and growing market. Even if great in theory, the process did not go very smoothly, with the translation of the regulation into national legislation taking up to 24 months in most of the countries and the Commission reporting the completion of the process only in October 1999. Moreover, the EU left, according to several experts, perhaps too much room in the implementation of these changes, leading to substantial implementation gaps between what had been theorized and what actually happened, even if this was done with the intent of creating a framework that would help all states, that proceeded at different speeds, to achieve the same results.

Despite these criticisms that are still object of discussion inside the scientific community, the process appears to be for the most part successful: in fact, where the market was once ruled by inefficient, state-owned monopolies that employed high prices and wouldn't produce innovation for the sake of better profits, the power from that point onwards shifted to the ends of the open market. In just a few years, many of operators had been privatized completely and entry had been liberalized, finally creating an open market. As a consequence, prices dropped significantly in all countries, and the telecom industry changed dramatically for the better, enabling the widespread diffusion of the Internet[19].

The key element to understand regarding the economics of the Internet backbone, infrastructure and services is that, even if the phenomenon may seem new on the

[19] Abbott, A. B. (1999). The Liberalization of the Telecommunications Sector: A Rent-Seeking Perspective. European Journal of Law and Economics, 63–77.

surface, it actually resembled a lot of the trends and mechanism that spurred during the telegraph and telephone era, at least during the early stages. The more digital technology converged towards the Internet, and the more digital video, audio, and generally interactive multimedia has grown in popularity and in use, the more we observed a shift towards a different economy system, where service providers such as Google or Amazon begun generating much higher revenues than the players that once ruled and managed the Internet, such as the old national telecommunication companies that actually built the infrastructures. This situation though creates real concerns in terms of power, that have been up for debate in regulatory actors such as the European Commission and Parliament for more than 20 years and that are now putting regulators in a new spot, that requires more regulation instead of liberalizations, a complete shift compared to the 1990's[20].

It's important to note that the examples discussed later will be both about the U.S. market and the European market, not because of lack of information regarding the EU side of the matter, but because of the importance and the impacts that the U.S. economic playground had on the European countries, that most of the time has undergone same or similar processes compared to the ones that had happened just a few years earlier in the United States.

The first of the aforementioned trends that makes the first economic developments of the Internet similar to the developments seen in earlier telecommunication history, relates to the impact of large firms and banks, which played an important role in the development and dissemination of all communication technologies, like the research of faster data transfer technologies. But why is such an obscure and complicated product of so much interest by so many actors?

When discussing the economic nature of the Internet, it is important to take into consideration the type of commodity that the Internet in itself is: in the words of

[20] Blayne Haggart, N. T. (2021). Power and Authority in Internet Governance: Return of the State? London: Routledge.

Hillis[21], being an invisible commodity, it is easier and more profitable to exchange it, particularly if we think about how the market is shaping nowadays, with more and more e-commerce sites, general services, entertainment services and financial services all based upon the technology, the inherent value of it just keeps growing. This is the reason why so many companies were attracted to the Internet even in the early stages, when profits still seemed small. This process, though, didn't start right away, and companies, particularly the big telecom organization that held monopolies in their respective national markets, were afraid of spending resources on a project that seemed very optimistic and ambitious, so they simply opted to stay out of trouble. In this regard, the U.S. case is very telling: until its dethroning in 1982, the main telecommunication monopolist in the U.S., AT&T, short for American Telephone and Telegraph Company, was in complete control of the market, with no chance for others to opt-in. In 1971, The Department of Defence asked them to take over the management ARPANET, but the company decided to decline the offer, unable to see the potential of the technology and unwilling to invest in the necessary infrastructures needed for packet switched networks. This was also due to the fact that they were asked to manage it as a public service, and AT&T thought that being publicly regulated the margins would have been lower and they would never have had the complete control over the network.

Taking a brief look at the supply side, research seems to underline drastic changes to the industry from the time of the liberalization and onwards. When the most important competitors were historically the service providers, once the Internet took its toll and started to become a widespread commodity, equipment producers started to become more and more central. Particularly, companies that produced access points, switches, routers and generally network components instead of the building and management of the network itself. A company like Cisco, for instance, is generating much higher revenues and it is pushing for more research and development intensive work compared to the old carriers such as British Telecom or Deutsche Telekom. This is due to the huge

[21] Hillis. (1998). On the margins: The invisibility of communications in geography. Progress in Human Geography, 543-566.

costs that these companies endured when building the backbone, the infrastructures and the technical side of the network[22].

This does not mean that these organization do not play a role in the current market and decision-making process. Organizations and banks, exactly like they had done in the 1870's with the construction of private telephone lines across the ocean towards Europe to transmit information and exchanging goods, were among the firsts to invest and push towards fibre-optic lines. As a result, the market and industrial structure of the Internet has been guided for a long time by the choices of the big telecommunication firms that invested early in the creation of backbone networks and infrastructures.

This is still somehow true nowadays, but it is expanding to companies that have a great deal of power in the service market, instead of the infrastructure market: many large firms that operate in the service side of the Internet, such as Microsoft, Apple, Amazon, and Facebook for instance are growing so much that they don't even use third-party infrastructures anymore, but instead all of them operate their own data centres along with the relative connections and networks. Some of them, like Google, even built exclusive backbone wiring lines to avoid leasing backbone lines from other telecommunication operators, in order to operate at a lower cost and to allocate higher bandwidth and performance to specific tasks when needed, dynamically balancing load and requests across different paths and lines in an independent way. The downside to this is that these giant companies are taking so much power in the market that they are becoming a threat for legislation and security. For instance, according to Bates et al.[23], these kinds of companies usually find scope economies across all the connected services, bundling them up to appeal to the end-user. The impact of this on the balance of power and the decision making can be quite significant, as we'll develop more in the later parts of the discussion. From a purely economic standpoint, large firms could hinder innovation, by sticking to proprietary protocols and processes that can't be used by other companies to develop newer products or technologies. That is why, in this field

[22] Tian, H. J. (2021). The Economic Impact of Internet Connectivity. INSEAD.
[23] Bates, S. J. (2018). In support of Internet entropy: mitigatin and increasingly dangerous lack of redundancy in DNS Resolution by Major Websites and Services. NBER Working Paper 24317.

particularly, legislation has come a long way to try to create standards, that actively force companies to adopt the same technologies and making the products talk with each other, to benefit end-users and those new companies who want to access the market.

1.5 The digital economy in the EU

After going over the historical characteristics of the Internet market and how the power shifted from the states to the private sector thanks to the liberalization process, it is useful to introduce the concept of digitalization, in order to better assess the great transformation that the advent of the Internet caused in the world economy, focussing on the particular case of the European Union. Again, some references to the world economy, mainly to the U.S. case, will prove useful to put the data into perspective.

Digitalisation, known as the diffusion of digital technologies, quickly led to the birth of the concept of digital economy, which represents the new way of conceiving the economy of the world based on the new interconnection tools that the Internet developments created in recent history. Billions of connections among people, businesses, data, and services that happen every day, undermining the conventional processes and notions related to organizations: it's peculiar that a business can be created without even physically owning the product sold. Think about the Uber case for instance, which became the biggest taxi company without owning a single vehicle, or eBay, which has no inventory, but it is still one of the biggest retailers in the world.

One thing is for certain, the transformation is inevitable, with economy experts unsure if this process will make the difference between developed and less developed countries more relevant[24].

[24] Milošević, N. e. (2018). Digital economy in Europe: Evaluation of countries' performances. Zb. rad. Ekon. fak. Rij., 861-880.

In terms of added value in the form of percentage of GDP, the U.S. lead the race of the digital revolution of the economy, as shown in Figure 6, with the European Union steadily following the same path of growth.

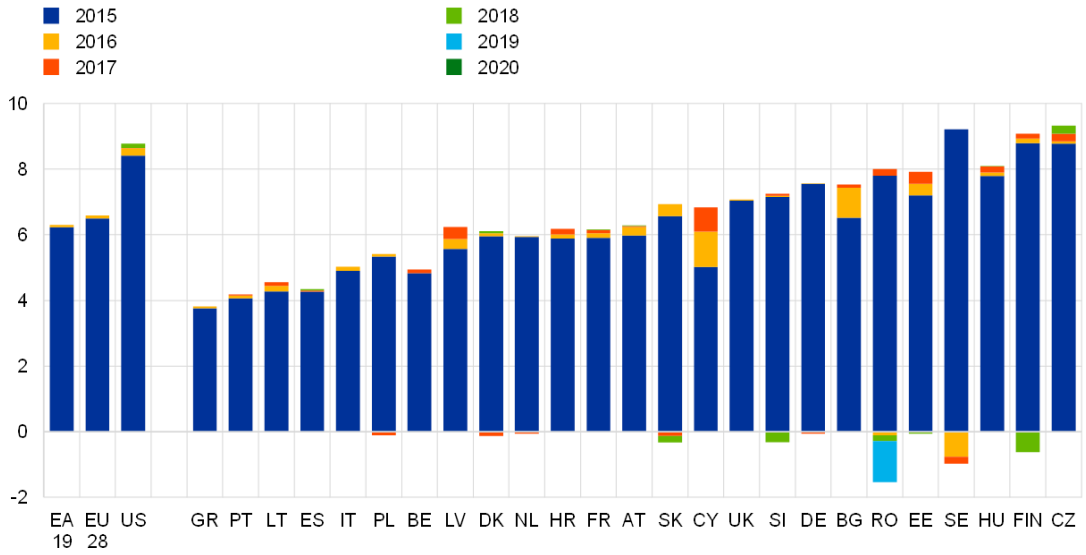

Figure 6, % of GDP, Source: European Commission.

The growth can be accessed more specifically taking into consideration the Digital Economy and Society Index. This document produced by the European Commission monitors, since 2014, member states' digital progress and publishes the result in this report. In Figure 7, the chart shows that even if there are differences in the European landscape, a clear and steady trend of progress is taking place.

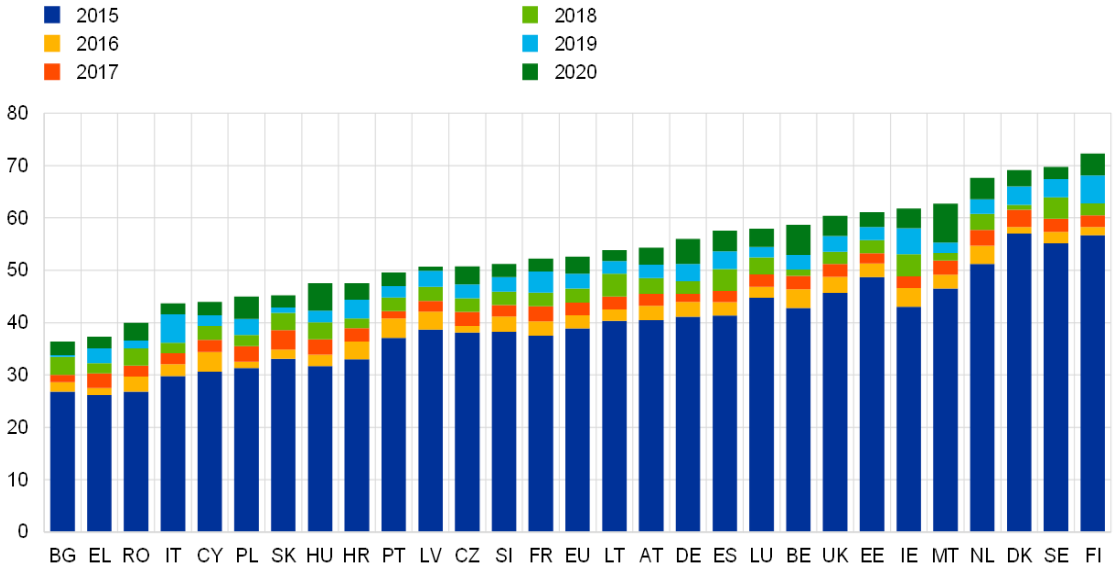

Figure 7, Digital Economy and Society Index, Source: European Commission

The thing to note is that, even if the broadband and general infrastructures related to the network have reached comparable levels in most countries of the European Union, there are differences in other aspects of the digital economy developments, such as the digitalisation of the public administrations, that is a necessary and proven tool, notably in current times where the COVID19 pandemic still poses a strong challenge to many sectors, to promote better education, health services and transports[25]. The so called "digital citizenship", which is the bag of online and digital services that every citizen is entitled to, is a necessary innovation, that provides quick access to data, documents and services that interest them and the attention towards it is growing.

Elements such as digital entrance to support free and unlimited access to all the provided online tools; digital communication, to be more connected with other people, at work and during daily tasks in life; digital skills, to always know how to use devices and how to access the needed information; digital commerce to provide access to food and basic commodities to the elderly or people with motor disabilities are all to be not only implemented in an efficient way – something with which countries in the European Union are struggling – but also regulated, to achieve a safe, fair and secure digital life, without the constant fear for privacy and security issues. This is a key discussion point that we will discuss in the second part of this analysis, and that requires the notion for E-Government, stated by the EU in a communication of September 2003[26]:

> "…the use of information and communication technologies in public administrations combined with organisational change and new skills in order to improve public services and democratic processes and strengthen support to public policies."

And its basic principles which were updated and stated during 2016 State of the Union, dated September 2016 and that regarded the planned actions for the time period 2016-2020[27]:

[25] Robert Anderton, V. J. (2020). The digital economy and the euro area. ECB Economic Bulletin.
[26] European Commission. (2003). The Role of eGovernment for Europe's Future [SEC(2003) 1038]. European Commission.

[27] European Commission. (2016). Commission paves the way for more and better internet connectivity for alla citizens and businesses. Strasbourg: European Commission Press Release.

> "By 2020, public administrations and public institutions in the European Union should be open, efficient, and inclusive, providing borderless, personalised, user-friendly, end-to-end digital public services to all citizens and businesses in the EU. Innovative approaches are used to design and deliver better services in line with the needs and demands of citizens and businesses. Public administrations use the opportunities offered by the new digital environment to facilitate their interactions with stakeholders and with each other".

As previously mentioned, the pandemic had a real impact on the EU's economy and society, leading to a push towards the digital state. This puts pressure on the related actors, that need to quickly adapt to a new way of operating, educating workers of the public administration and pushing for investments thanks to the funds – Recovery and Resilience plans - that the Union put in place to comeback from the big crisis caused by the pandemic. The DESI 2021 report, to measure the digitalization targets and dimensions, is divided in 4 main components shown in this table taken from the aforementioned report:

1 Human capital	At least basic digital skills ICT specialists Female ICT specialists
2 Connectivity	Gigabit for everyone (Fixed very high capacity network coverage) 5G coverage
3 Integration of digital technology	SMEs with a basic level of digital intensity AI Cloud Big data
4 Digital public services	Digital public services for citizens Digital public services for businesses

Figure 8. Digital Compass targets used in DESI 2021. Source: European Commission

Taking a closer look at the sectors, human capital is the first one taken into consideration, and it is related to digital skills and ICT specialists as well as female presence among the ICT specialist category. In terms of digital skills, even though 84% of the population regularly connected to the Internet, just over half of them has basic digital skills. The worrying sign here is the growth rate, which appears to be minimum from 2015, scoring a mere 0,9% of annual increase: this means that people that stayed away from Internet related services does not get the right incentives to start using these

tools, and prefer to delegate mandatory tasks to friends, family or specialists with the right competences.

ICT specialist is a rare category, hard to come by, at least in regards of the EU market. European Union data shows that 55% of companies that recruited or tried to recruit ICT specialists reportedly struggled to find new workers, with areas such as cybersecurity, and data analysis still being filled with vacancies. According to the same data, businesses lack staff with adequate digital skills, making it hard to invest. Moreover, the gender ratio is 1 to 3, meaning only one in three engineers, science, technology, or mathematic professionals is female.

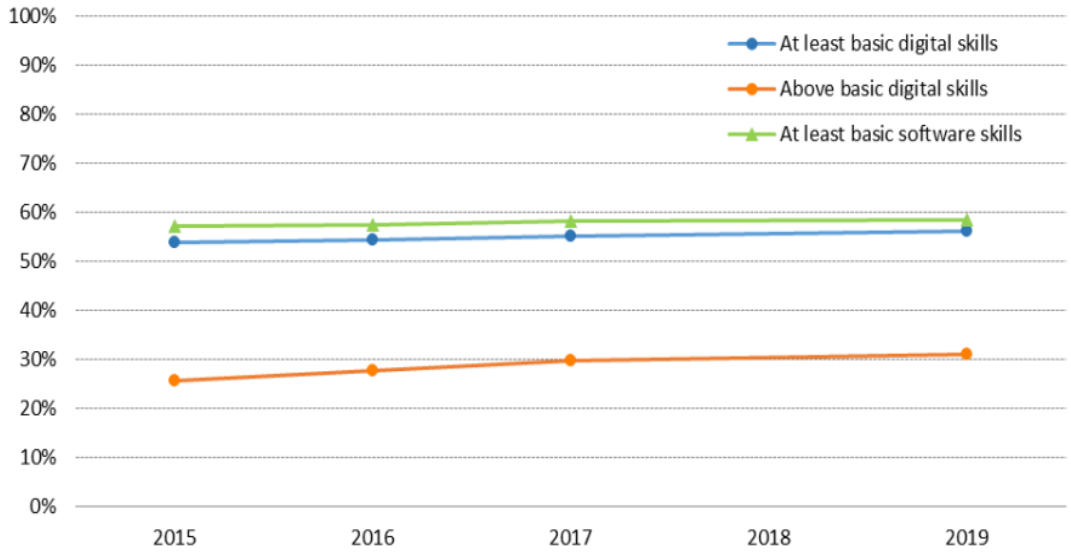

Figure 9. Percentage of digital skills, individuals. Source: Eurostat, sourced by DESI 2021 p. 15.

We'll be discussing 5G coverage and development in a later segment, but for what concerns the current situation of fixed, very high-capacity network (VHCN) with at least 1Gbps speed is still uncommon with only 1.3% of European families having access to such a high-speed connection. On the contrary, the general data for the spread of the infrastructure is positive meaning that the trend is going upwards, and more and more EU citizens can access better and better connectivity based on fibre optics at least in its FTTP form – fibre-to-the-premises (the form where a fibre optics cable reaches the ISP premise and not the directly the home of the user, like with FTTH).

Taking into consideration the third point of the analysis, the one about integration of digital technology by businesses, we see that the European Union has very different results depending on the area taken into consideration. For instance, northern countries such as Denmark and Finland rank very high with numbers close to 90% of organizations that reach a sufficient level of digitalization, while countries of Eastern Europe, such as Romania and Bulgaria only scoring 33%, with most countries sitting around half of the businesses having adopted enough digital and Internet related technology and services. Generally, small and medium-sized organizations lag behind bigger companies, particularly in terms of the more advanced Internet technology such as AI, Cloud and Big Data, due to the inherent costs of hiring experts and the long periods of time required to effectively integrate these new and advanced technologies in the existing methods, infrastructures and workplaces.

Unsurprisingly, northern European countries, particularly Sweden, Finland and Denmark are leaders in terms of digitalization and digital adoption of services from businesses.

We've already mentioned the e-government and digital public services, noting that they are getting better in terms of data, even if the actual use by citizens around the EU still sits at 64%, just a 6% increment from the data from 2015. The biggest gap still stands in the use of the more advanced technologies, such as the beforementioned Cloud, AI and robotics and Big Data fields: these services could theoretically improve the daily life of citizens and public administrations by a good margin, but data shows that big investments are still needed in this direction. Moreover, progress seems very different from country to country in the EU in terms of public administrations digitalization levels, with the need for much more work in terms of funding, research and awareness.

The report ends with a general performance meter that puts into perspective the levels of digitalisation across all European Union members, that confirms then general trends we've observed so far:

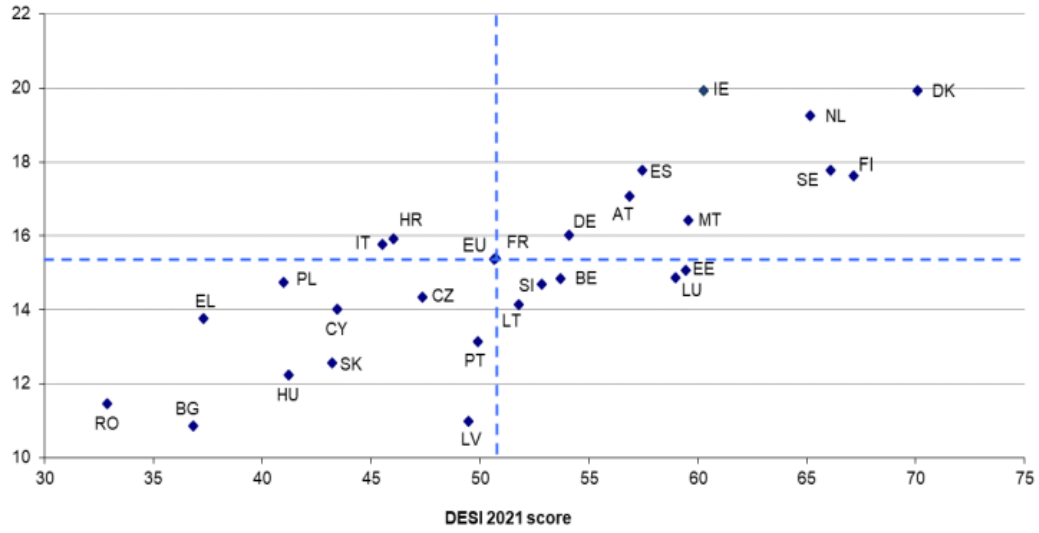

Figure 10. DESI 2021 - EU Member State's scores in the period 2016 - 2021. Source: DESI 2021, European Commission

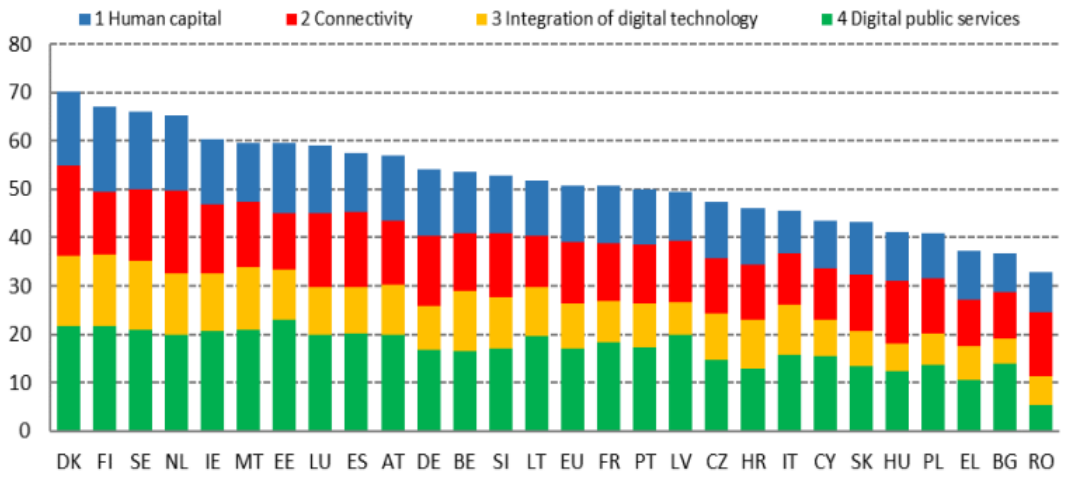

Figure 11. DESI 2021 score sorted by categories. Source: DESI 2021, European Commission

Other economic implications: productivity

Discussing productivity in regard to digitalization is more complex, because in the last few decades production has experienced a decline, with lower levels of total factor productivity, that started way before the financial crisis of 2009. This is notable, particularly because the sectors that are more prone to this productivity deceleration are the once relying the most on information and communication technology (ICT). Economists argue that this happened because the new digital economy is still in a

"installation phase" and will eventually be followed by a "deployment phase"[28]. The installation phase is characterised by the exploration of the new markets and possibilities, with new technologies being developed at a faster rate and greater research and development spendings. Success cases during this phase often cause a mushroom effect, with a huge number of new companies entering the market: a process that eventually leads to many organizations and start-ups to fail. This is usually followed by a frenzy period, that again is followed by the beforementioned deployment phase, when the technology becomes widespread, mature, and cheap enough that it can be more easily accessed by buyers. This phase is the most profitable moment, and helps lowering costs, thus leading to higher levels of productivity, and levels income[29].

Comparing the European economy to the U.S. one, economists have also observed that the latter was able, during the 90's, to increase productivity in the same information and communication technology centred fields where the EU struggled: the European Union study case lagging behind in both development and deployment of Internet-based technologies, even if seemingly there were no big difference to the actors and the economic scenario.

The hypothesis of the possible causes of these developments are many, but the most notable ones argue that it could have been caused by the lack of adaptation to the new processes, methods, and technologies, as well as a generalized lack of qualified workers. The more flexible and decentralised structure of U.S. firms has played a role as well according to Bloom et al.[30], a trend that appears to be present among different United States companies as well. Most of the research seems to argue that there's a clear positive trend among those companies that embraced modern management practices, such as providing good feedback, improving communication, and creating a good

[28] Ark, B. v. (2016). The Productivity Paradox of the New Digital Economy. International Productivity Monitor, 3-18.
[29] Harberger, A. C. (1998). A Vision of the growth process. American Economic Review, Vol. 88, No. 1, 1-30.
[30] Bloom, N. B.-E. (2019). What Drives Differences in Management Practices? American Economic Review, Vol. 109, No 5,, 1648-1680.

working environment. These companies generally experienced better results in terms of productivity, as confirmed by Andrews, D. et al.[31] in a recent study.

The same source opened to another critical issue of new Internet-based technologies, regarding the hardships in terms of adoption of these tools, showing how the policy environment can greatly affect the results in terms of digitalization. We'll dig deeper on this topic in later parts of this analysis, going over the European Union framework regarding telecommunication and Internet policies.

Another Internet related point of the digital economy that needs stressing is the difference between fixed and mobile connections, and what is the market direction in the EU, and in the global spectrum. Fixed connections, along with telephony, have experienced a major decline in the past 15 years, worldwide. It doesn't matter if we're taking into considerations developed countries or developing countries, the trend is clear and coincides with the spread of cheap mobile phones and Internet subscriptions.

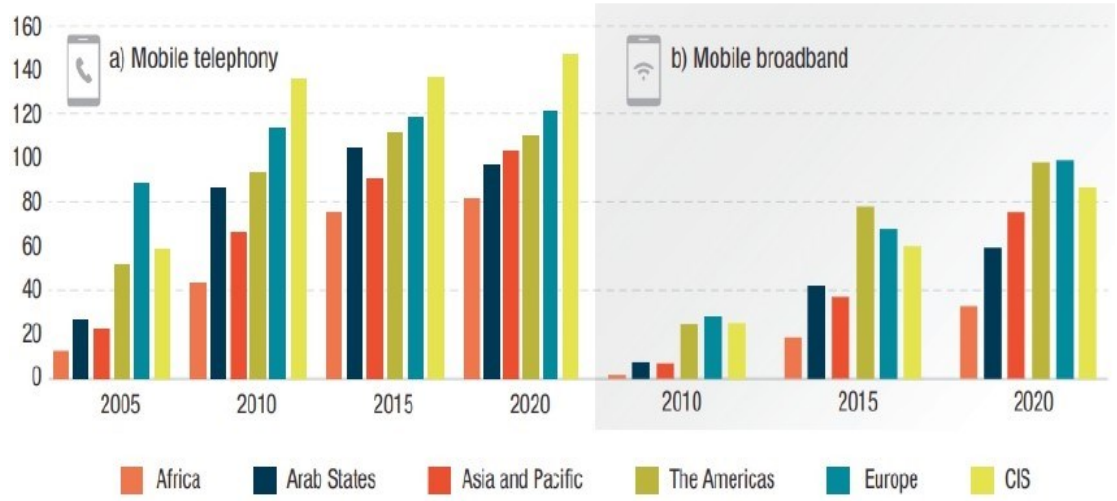

Figure 12. Mobile telephony and broadband subscriptions (per 100 people).

Source: UNCTAD, based on ITU Statistics database, available at www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

Europe and America lead the development with numbers, that, already in 2020, reached the 100 subscriptions per 100 people, effectively showing that Internet has become a part of everybody's life in the two more advanced parts of the world. This is closely link to the development of 3G, 4G and 5G mobile connection technologies: while 3G

[31] Andrews, D. C. (2019). The Best versus the Rest: Divergence across Firms during the Global Productivity Slowdown. Mimeo.

network is the standard nowadays, with 93% of the world being covered by this type of signal, 5G is seeing great investments because of its strong implications in various key sectors, such as data and communication, but also health and administration.

5G and its economic implications in the digital economy

5G connection is considered by many economists and experts of the digital market as the real transformer of the following years. Let's take the workplace as an example, to better understand the implications of 5G. For starters, thanks to unprecedented download and upload speed numbers, that also allow for low latencies, workers could literally bring the workplace wherever they need. This translates into a more flexible and connected workplace, that is linked by many studies such as early as the 70s to increased productivity and general workforce wellbeing[32]. This topic gets more and more relevant in the present time, with companies employing newer and more modern techniques to try and fight the settle backs created by the pandemic, such as smart working, and cloud-based solutions.

To understand the scale of this technology and particularly where we are in terms of adoption worldwide, we can use the following chart taken from Statista and sourced by GSMA.

[32] Schein, V. E. (1977). Impact of flexible working hours on productivity. Journal of applied psychology, 460-467.

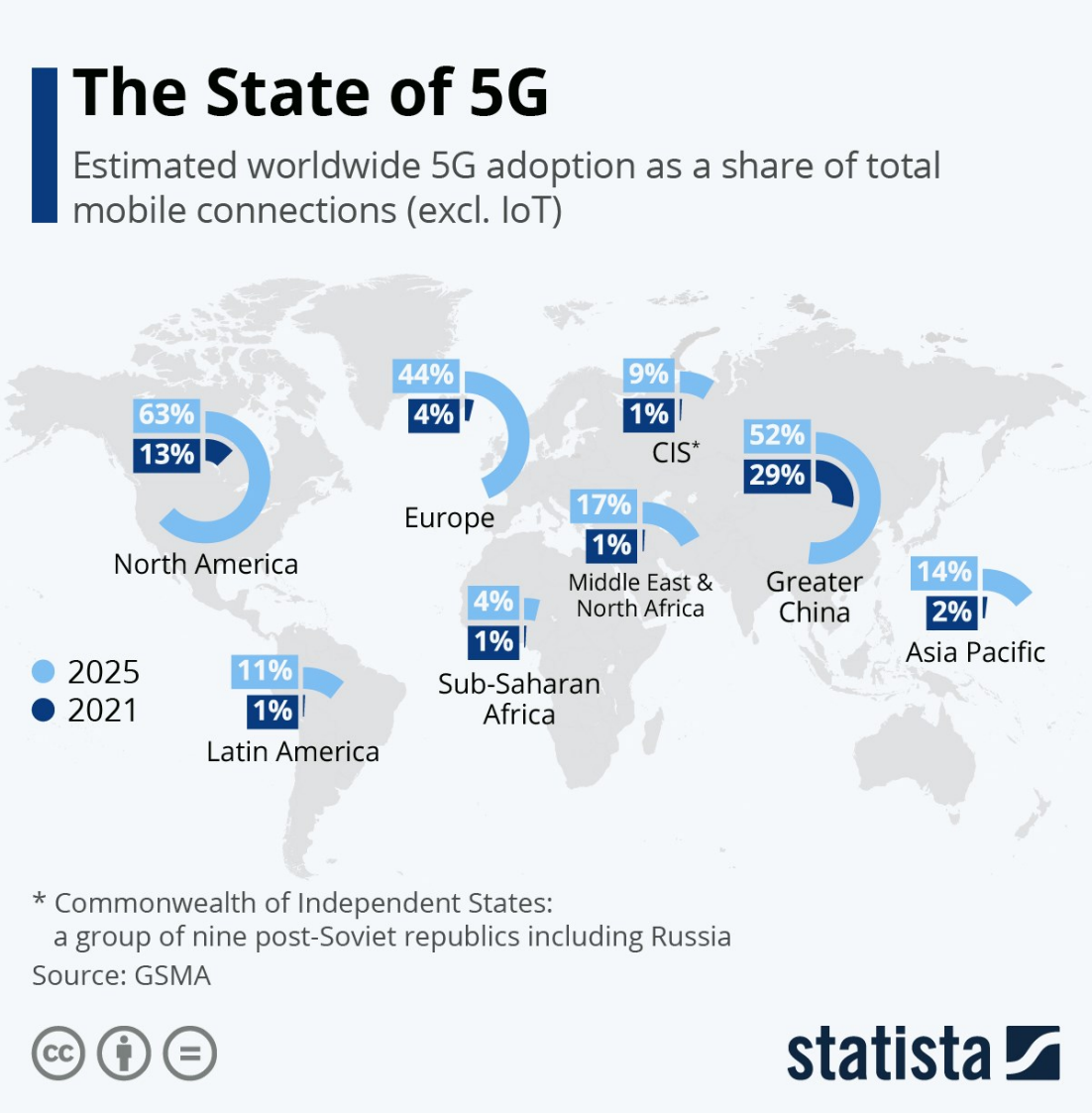

Figure 13. The State of 5G adoption worldwide. Source: GSMA

According to the GSMA, in 2021 5G accounted for 8% of all global connections, with huge differences in terms of areas of interest: Greater China is undoubtely the area with the biggest adoption, with 29% of all mobile connections already relying on the newest techology. The difference with Nord America is quite remarkable, seeing that historically, this area has dominated the race in terms of adoption of new telecommunication and Internet standards. In fact, the expected adoption by 2025 seems to resemble more the general trend of development, with Nord America taking the lead back and Europe drastically rising its adoption rate with a huge increase from 4% to 44%. As expected, developing countries will still heavily rely on 4G and 3G technologies, at least in the next following years.

The whole value chain of mobile broadband is currently experiencing the consequences of the deployment of 5G technology. This means that companies inside the value chain provide a direct economic impact, in the form of the investments that organizations are making. The global 5G value chain contribution, measured by the team of HIS Markit using standard input – output analysis techniques, reveals that the share of 5G value chain R&D is only going to grow from 2020 to 2035, with some of the biggest countries in the world including Germany, U.S., France, and the UK averaging over $200 billion of investments annually. Of course, the investments in this regard will go down once the infrastructures are built and the attention will be shifted into the development of application, services and tools to really benefit from the use of this technology[33].

The core keynote here is that 5G is a long game, that has to be played with attention: making the right investments while creating the perfect policy environment for its capabilities to be exploited is a key discussion that the European Union has to face. Challenges such as avoiding security vulnerabilities, increased attacks, confidentiality and privacy threats, limited experts on the matter and supply chain related risks, are all to be discussed before-hand, to ensure a safe widespread deployment of such technologies in the future and in the present time.

Developments of modern Internet economics: cryptocurrency

One of the core issues of digitalization is that we can never understand it well enough that it has already evolved into something even more complex and different, and this happens really quickly. This, combined with the sheer complexity of the system of services that the Internet produced nowadays, leads to potentially dangerous and hard to control services or software to spread. Cryptocurrency, for instance, is a great topic of discussion and research, and it will take a few years for policy makers to fully grasp this new tool. How well can this new currency serve as a tool for payments, is a question that many economists and policy makers are asking themselves nowadays, with

[33] Campbell, D. F. (January 2017). The 5G economy: how 5g technology will contribute to the global economy. IHS Economics & IHS Technology.

economists and researchers arguing, or even denouncing, cryptocurrencies as unreliable and shady tools to support illegal activities or creating economic bubbles to exploit quick earnings.

The very first online currency based on the blockchain system was the Bitcoin. To grasp the full spectrum of what this technology is and how far reaching the developments of the Internet have been in terms of services, infrastructures and innovations, we must refer to the original paper named "Bitcoin: a Peer-to-Peer electronic cash system" by Satoshi Nakamoto[34] published in 2008, that backed up the creation and publication of the website bitcoin.org, registered in the August of 2008. The author strongly criticized the current process of electronic payment processing, assessing how third parties couldn't always be trusted in overseeing and ensuring these procedures, that dealt with advanced encryption, would always be safe and fast. This also introduces financial costs, because of the needed involvement of third parties. To solve this issue, he developed a system in which electronic payments are based on cryptographic proof instead of just trust, allowing for direct transactions through a cryptographic system. Nowadays, many of these virtual currencies are distributed online, and usually live in the form of decentralized networks based on the blockchain technology. The blockchain is what allows for cryptocurrency to exists as secured and decentralized when a as transaction occurs: a distributed database shared between the nodes of a computer network, just like it was in the early days of the Internet, but with data organized in blocks that hold sets of information. These blocks, that play the role of bookkeepers, store the exact time stamp and details of the transaction in the case of cryptocurrencies, with all data kept safe by cryptography techniques[35].

[34] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
[35] Er. Puneet, E. D. (July-Aug 2017). Cryptocurrency: Trends, Perspectives and Challenges. International Journal of Trend in Research and Development, Volume 4, 4-6.

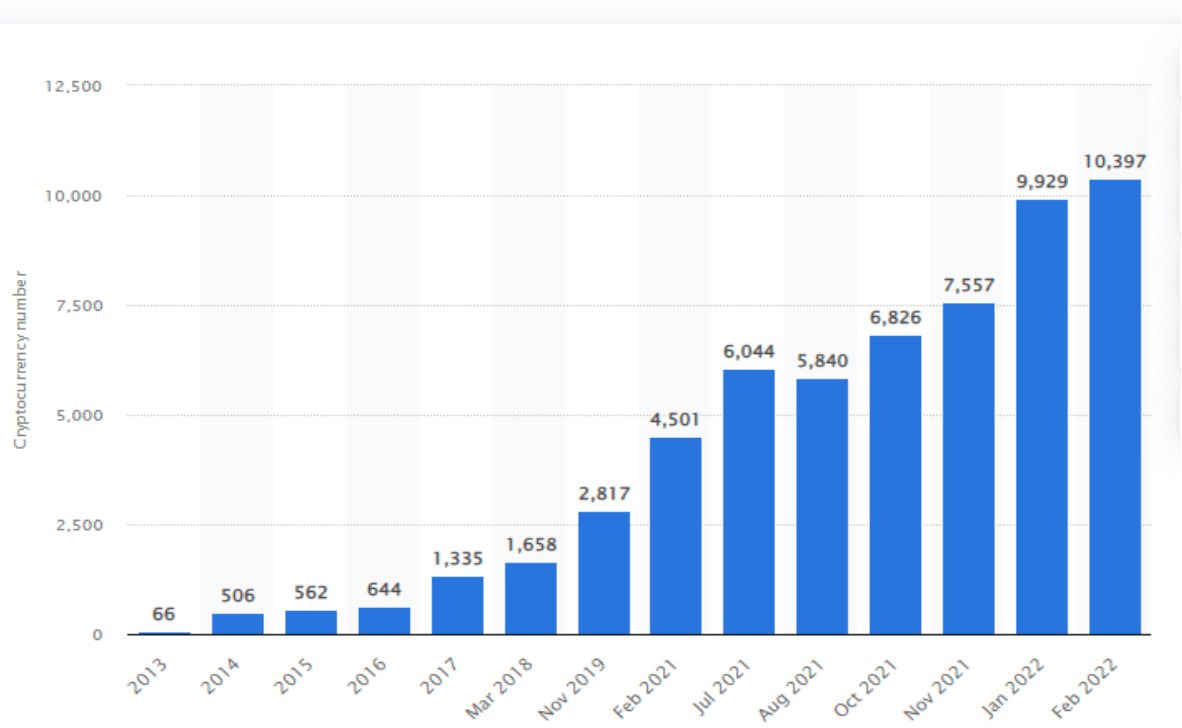

Figure 14. Number of Cryptocurrencies 2013 - 2022. Sources: 2013 to 2017 GP Bullhound .

According to the following graph taken from Statista.com, displayed in Figure 9, the number of cryptocurrencies worldwide spiked in 2021, reaching the five digits in February 2022. Since it is extremely simple to create a new currency, a great number of new coins entered the market, usually released to the public just to speculate on the initial "boom" that occurs due to people's curiosity and will to bet some of their money onto the next Bitcoin or Ethereum. Note that the top 20 cryptocurrencies represent 90% of the whole market. This fully digital currency could and is changing world economy as we know it, but just like the Internet in its early days, companies and governments are approaching it very slowly, most of the time not even acknowledging it or underplaying its value. Big companies are exploiting the knowledge gap of institutions through heavy lobbying, an issue that we will deal with in the third chapter of this essay.

1.6 The impact of the Internet on economic growth and prosperity

After taking going over the general digital economy and its implications, it is important to understand how the Internet directly impacted prosperity and economic growth. Taking into consideration world-wide performance, before 2009 the growth in GDP caused by the Internet accounts for 1,672 billion, that equates to 2.9 percent of total GDP. Significant growth was experienced in all the advanced economies such as the G8 countries, but also in middle of the road countries in terms of GDP per capita globally, such as Turkey and Mexico, the Internet appears to have contributed to foster economic growth.

The impact of the Internet does not only relate to the economy itself, but there's also a definite connection between how developed Internet networks and infrastructures are, and how deep they are embedded into the daily life of the population and living standards. These correlations appear to be even stronger when discussing developing countries, leading to the conclusion that the Internet, at least in its current phase, could work as an equalizer for countries in need, if backed by a strong policy framework.

In terms of the actors that benefitted more of the advent of the Internet, it appears that consumers and entrepreneurs are the players that achieved the most results. But this doesn't mean that the Internet hasn't benefitted organizations: in fact, SMEs and start-ups found in the new interconnected economy a chance to become instantly a global actor, when just a few years before such a position would have been impossible to achieve without huge investments. This level the plain field with the bigger companies that already had developed far-reaching connections: it became easier to find suppliers, reach customers, analyse the market, and collaborate with highly specialized and trained workers and researchers from all over the world.

As it was mentioned earlier though, the consumers are the category that seems to have benefitted the most from Internet's growth: this is due to the new tools that have been developed through the years, such as websites to compare prices and to access sales easily, platforms to access the property market or the vehicle market without the

need of third-party figures such as dealers and brokers, and generally better transparency. Data suggests that there is a correlation between users visiting website that compare prices and actual prices going down, with online prices being already, on average, 10 percent cheaper compared to off the shelf, physical goods[36]. Moreover, national health care systems and public administrations are more efficient thanks to digital services, with population general experiencing an improvement in their quality of life.

Economists, generally see the future of the Internet in terms of growth and prosperity in a good light. Research shows that a strong Internet based ecosystem enables countries to improve greatly during in many aspects of the economy, including better competition, a more open market, improved human capital and infrastructures. Productivity can be improved entering the "deployment phase" (Harberger, 1998) as we mentioned earlier, fully embracing new tech and the change that derives from it: the improvements in competition and the openness of the markets contributes to a faster and healthier economy. All of this strongly depends on the policies that decision makers deploy though: innovation for instance, only grows in an environment that grants start-up capital to new companies, is able to protect intellectual propriety, and constantly supports research and development. After all, if the United States wouldn't have pushed for innovation and granted funds to ARPA, we wouldn't be discussing about Internet technologies at all. The U.S. has generally been ahead of the curve in deploying new technologies, quickly creating skilled workers and human capital, working as an example worldwide on how to adapt and foster the creation of new companies.

[36] Bughin, J. (2011). The impact of Internet technologies: Search. Chicago: McKinsey & Company.

1.7 History and economics: a necessary background

This analysis of the economics and history of the Internet showed not only how important this new technology is for the EU and global economy but has also raised many issues and discussion points that are crucial to better regulate and manage the future of the digital world. In fact, it has emerged numerous times that regulators are the ones that influence and decide how deeply the Internet enters our daily life. Regulators are in charge of defining the implications of the connected and smart world and need to tailor solutions that allow people to remain free and safe while interfacing with all sorts of new online technologies that are slowly but surely entering the market and thus the daily life of customers all around the world, and particularly Europe.

Knowing the history and the general economic principles is a necessary step to grasp the reasons behind the decisions and the policies that the European Union is implementing and has implemented in the past to ensure that the economy develops and that key values such as privacy, freedom and security are safe. It stands clear that without a strong collaboration among policy makers and businesses, the development of a safe ecosystem of services and markets is impossible. This is why, to better understand what comes next in terms of digitalization and the issues that the regulators are facing, we'll analyse, describe and comment the current policy situation in the European Union, assessing how the decision made in this time period could be crucial in the following years in terms of safety, privacy and economic stability.

2. EU Internet and digital Policy: an overview

Internet and digital law and policy is one that keeps changing: in fact, the more discoveries and technological advancements are made, the more the legislative implications grow, making it harder and harder to grant equal, secure, and controlled access to these new solutions and services. The European Union, in this context, produces every year new frameworks and pieces of law to try and tame the digital beast: copyright, data protection, consumer protection, e-commerce regulation, big data and Tech Giants, are just some of the topics that are regularly and heavily discussed. Notable interventions by the EU in terms of cybercrime, dealt with cyber-attacks, online fraud, hate speech, unfair practices, and child pornography, which are topics that generally are received well by all parts, being lobbyists, companies and of course, members of the European Commission and European Parliament. But most of the time, these new topics become very relevant very quickly, with multiple actors such as lobbyists, NGOs and Think Tanks usually working for those giant companies that can afford to spend millions in this endeavour, making the difference in the decision-making process inside the EU[37].

To think that the European Union is just a single entity that can take quick and direct decisions, guided by a single interest which is the one of the European institutions is preposterous. The EU is a multi-level entity that by nature represents many people, and therefore relies on many institutions, offices, and people to develop different policies. This means that, throughout the years, all sorts of interest bearers have influenced the institutions providing knowledge, people's consensus, and data to support their claims: these interests have the ability to shape legislation at the core, during the very process that creates these policies and influencing the very actors that are supposed to work on these topics.

The process, commonly known as lobbying, is nothing new, particularly for the U.S. government and institutions: in fact, this way of carrying private interests towards the

[37] Lehmann, W. (2003). Lobbying in the European Union: current rules and practices. Luxembourg: European Parliament.

institutions is part of the U.S culture and the historical way of dealing with policy. Because of the relatively young age of the EU, lobbying is considered a newer process, that has flourished in the last 20 years.

The lobbying has involved all three main EU institutions, in particular:

- The European Parliament: being made from representatives that usually lack expertise and knowledge of all specific topics of discussion, this institution has been at the centre of heavy lobbying. Moreover, the lack of transparency caused by the current rules that do not render mandatory the mention of meetings with stakeholders, makes the process even easier and harder to monitor from the inefficient monitoring system currently in place. Even if attempts were made to introduce a legal framework from 2007 to 2015 requiring in particular rapporteurs, that are the actors at the centre of a committee that actively legislates on particular subjects, to report all the stakeholders consulted during the preparation of the report, the nature of this report is still voluntaristic, making it completely unreliable.
- The European Commission: the main vulnerability of the European Commission is its size. With so many offices, committees and people working for it, it's easy to bring interest into this entity: it's the committees, in particular, that see the most lobbying action, because of the key role in the legislation process, working as gatekeepers to new policy. Stakeholders bring the knowledge to get the committees up to speed, and at the same time on their side.
- The European Council: this institution has no regulations at all in terms of lobbying, and works closely with the EP, making it an easy target for stakeholders[38].

[38]Farrand, B. (2015). Lobbying and Lawmaking in the European Union: The Development of Copyright Law and the Rejection of the Anti–Counterfeiting Trade Agreement. Oxford Journal of Legal Studies, pp. 487-514.

At the core of this lobbyist push, we can undoubtedly put the big tech companies. Particularly the big five of the tech industry, Google, Amazon, Meta (formerly Facebook), Microsoft and Apple, have spent 19 million on lobbying European institutions in 2020, Google leading the pack with 6 million spent in just a year[39]. These amounts of money are simply outstanding and unseen: in fact, comparing these numbers with the car industry. Europe's seven biggest car manufactures - Volkswagen, Daimler, BMW, Renault, Ford, Fiat Chrysler, and Peugeot – have spent a total of 7.9 million euros on lobbying in 2019, which represents half of what the tech industry spent.

The latest data on lobbying sourced by the transparency register shows that these numbers kept increasing between 2020 and 2021, with the discussion on the Digital Services Act and the Digital Markets act being very important for the future position of tech behemoths on the market.

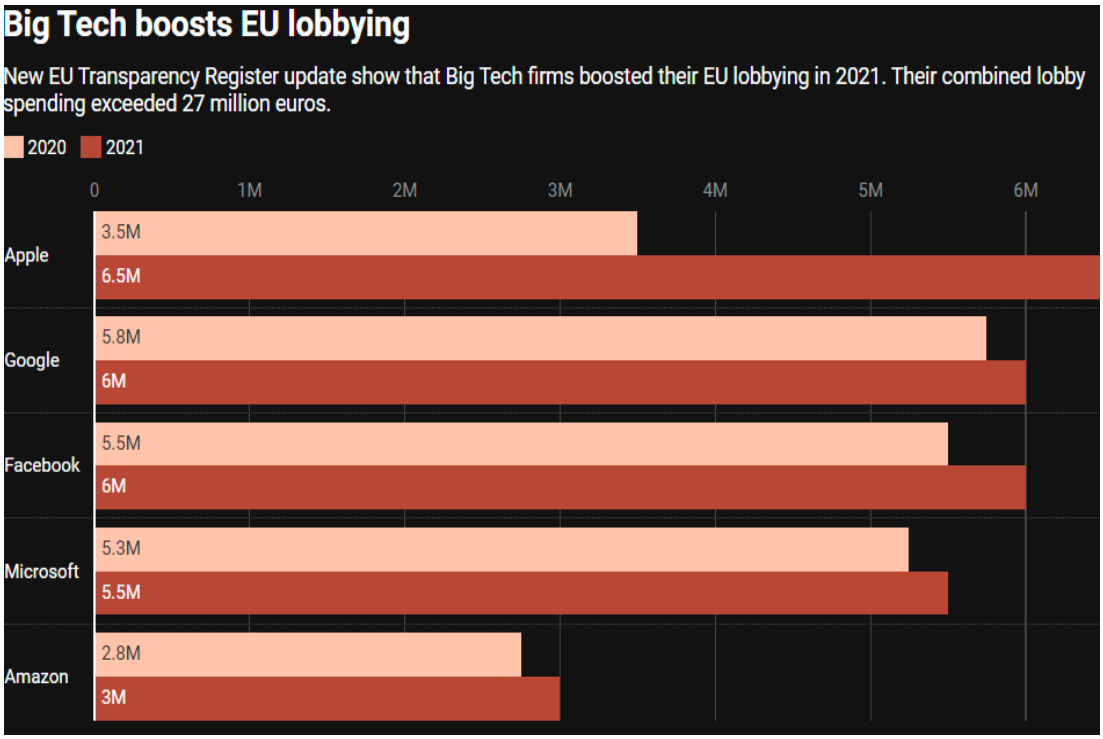

Figure 15. Big Tech lobbying in the EU, 2021 data. Source from EU transparency register Dec 2021

[39] Kergueno, R. (2021). Deep pockets, Open Doors. Big tech lobbying in Brussels. Brussels: Transparency International EU.

Regarding lobbying in the EU when discussing digital privacy issues already in 2013, former EU commissioner Viviane Reding mentioned that:

> "The lobbying from all sides has been fierce – absolutely fierce – I have not seen such a heavy lobbying operation[40]."

Generally, we can observe a clear concern by the EU on the topic, but a lack of action. The lack of accountability and oversight create a policy environment that struggles to identify solutions and come up with ideas without external influence.

This idea has to do with a concept we stressed multiple times in this writing: such a new and everchanging field, of which implications are so hard to comprehend by a non-expert, will always be more prone to external influence, due to the strong interest behind companies. These organizations hire the most experienced people, gaining a big advantage over institutions that have to deal with several issues at a time, and cannot afford to stay up to date dedicating so much time and resources. Moreover, there is a gap that needs to be filled at the national level: member states need to be up to date to make the best decisions for national policy, that usually works as a framework for the European Union policies to slot in, playing an important role in the implementation phase of these policies.

[40] https://www.telegraph.co.uk/technology/news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.html.

2.1 The relevant actors in the decision-making process

When discussing the internal and external European Union legal framework related to the digital and Internet field, there are a number of actors and stakeholders, other than the main institutions of the EU, that play an important role in taking decisions and discussing policy. It is important to assess their specific role in order to better understand why and how particular decisions are taken.

The Directorate-General for Communications Networks, Content and Technology

Established by the Barroso II Commission in 2012, the DG Connect was rebuilt from the former DG known as *information society and media*. This happened because of the need for new tools and policies to deal with the upcoming technological advancements. Citing the former website page for the information society and media DG[41], we can consult the mission of this new entity:

> "Support the kind of high-quality research & innovation which delivers imaginative, practical and value-enhancing results;
>
> 1) Foster creativity through a European data value-chain in which anyone can share knowledge;
>
> 2) Promote greater use of, and public access to, digital goods and digital services, including "cloud" computing, in order to boost the European single market;
>
> 3) Ensure that those goods and services are more secure, that people can trust the rapidly evolving technologies which surround them, and that people have the right skills and confidence to use them as part of everyday life;
>
> 4) Work with partners globally to support an open Internet."

The DG is the main body responsible for the development, creation and management of the Digital Single Market. In fact, the DG is composed by many sub directorates, each one taking care of a specific branch of the digital world[42]:

1) Connect A: artificial intelligence and digital industry;
2) Connect B: connectivity;

[41] https://web.archive.org/web/20120609074456/

[42] http://ec.europa.eu/dgs/information_society/connect_en.htm

3) Connect C: digital excellence and science infrastructure;
4) Connect D: policy strategy and outreach;
5) Connect E: future networks;
6) Connect F: digital transformation;
7) Connect G: data;
8) Connect H: digital society, trust and cybersecurity;
9) Connect I: media policy;
10) Connect R: resources and support.

The Committee of the Regions (CoR) and the European Economic and Social Committee (EESC)

These two consultative bodies work in close relation to the institutions to advice and bring the interests of different actors outside the EU, and they play a key role in the decision-making process, even if their suggestions are non-binding. The CoR is describe in the official website as: "…the voice of regions and cities in the European Union (EU). It represents local and regional authorities across the European Union and advises on new laws that have an impact on regions and cities (70% of all EU legislation)[43]." Made from 329 members and 329 alternates coming from all member states, the body aims at involving local and regional interests in the legislative process, helping with the objective of coordinating effectively the multi-level governance system that the EU put in place.

The EESC is a more specialized body that is: "Committed to European integration, the EESC contributes to strengthening the democratic legitimacy and effectiveness of the European Union by enabling civil society organisations from the Member States to express their views at European level.[44]" The committee helps not only to make more informed and efficient decisions in terms of "democratic legitimacy and effectiveness" but also aims at promoting the concept of a more participatory EU, closer to the population and the values of European integration. This body was conceptualized in 1957 within the Treaty of Rome and its consultation is mostly optional, with some cases in which it is mandatory.

It is important to mention that both CoR and EESC suggestions happen during the whole decision-making process of the EU, with these committees dealing with all the main institutions.

Other actors and stakeholders

Apart from actors that operate internally in the EU and the lobby groups, national parties, governments, and organizations also play a role during the process. This depends heavily on the type of legislation discussed, but the nature of the multi-level

[43] https://cor.europa.eu/en/about/Pages/default.aspx
[44] https://www.eesc.europa.eu/en/about

governance system makes it that directives need to be implemented in each member state's national law within certain time frames. As we've already mentioned, this process can be slow: in fact, even if the Commission has tools to punish the non-complying members, this inevitably slow down the implementation, a problem that can seriously hinder the competitiveness of the EU when talking about innovative and modern technology.

2.2 Policy and legislation regarding the digital economy during the Juncker Administration: The Digital Single Market (DSM)

The Juncker Administration operated in probably the most important time frame for the development of the digital economy and digitalization in general, leading the EU from 2014 to 2019: in fact, during his first State of the Union speech[45], which is the annual speech addressed by the leading president of the European Commission in front of the European Parliament plenary session in September, he marked the EU priorities for the following year in terms of legislation and policy. Among other relevant topics, such as refugees and immigration, Brexit, and climate change, President Juncker underlined the need for a so called "Digital Single Market" strategy, to ensure to all people of the EU high speed access to online services and tools, granting fair trade and competitive advantages to companies and organizations willing to invest in the EU framework.

In fact, the key elements of the Digital Single Market (DSM) policy package are the following:

1) Improving access to digital goods and services, leading to free access of goods among actors in the EU environment, leading to better competitiveness while at the same time ensuring that online business work in the provided legislative framework, removing all possible "grey areas";
2) Creating an environment where digital innovation, solutions and services can grow and prosper, by providing infrastructures that are not only fast and based on the latest technologies, such as fibre-optics with speeds of at least 100Mbps, but that are also safe and secure, taking care of issues such as data privacy and data protection, cybersecurity, fairness and transparency of e-commerce and online platforms in general;
3) Making it so that online and Internet related services are more accessible to everybody, improving the digital skills of European Union's citizens are always

[45] https://ec.europa.eu/info/priorities/state-union-speeches/state-union-2015_en

up to date, to exploit the value of these services and create a more equal and connected world (European Commission, 2015).

We'll now take a closer look at all the directives and regulations that made possible the creation and Digital Single Market strategy and policy package sourcing from the European Parliament list of policies[46], in order to analyse the policies in relation to the economic and historical context we've previously described, to later assess their effectiveness – if possible – and discuss possible issues or ideas to do better in the future using the available data. Before going over with the list, it has to be noted that directives and regulations are different legal acts or types of legislation that the EU can use. There are in fact five types of legislation from the most binding to the less binding according to the EU official website[47]:

1. *Regulations:* Binding legislative act that must be applied in its entirety across the EU.
2. *Directives:* Legislative act that sets an objective for all EU member to achieve. It's up to the individual country to produce and manage the laws involved to achieve such goals.
3. *Decisions:* "Binding to those to whom it is addressed".
4. *Recommendations:* Non-binding, serves as a way to make the EU view known to countries and to suggest a line of action without any official legal requirement.
5. *Opinions:* Non-binding instrument, is used to share viewpoints upon specific topic, particularly the opinions of specific committees that carry particular interests.

[46] https://oeil.secure.europarl.europa.eu/oeil/search/search.do?searchTab=y
[47] https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en

2.3 Key Directives

Directive on the certain value added tax (VAT) obligations for supplies of services and distance sales of goods – 2017/2455[48]

Key Action number 8 of the DSM includes the application of reliable VAT rules in the context of e-commerce and online marketplaces. The issue had been discussed for many years, and it revolved around the fact that there are a number of different VAT and tax systems among the different Member States and also outside the EU. The decision of modernizing cross-border rules in terms of VAT application for both businesses and consumers was not an unforeseen one, with the plan for a one-stop shop portal that helps businesses comply correctly with the VAT obligations: the problem was that for each other country in which an online store wanted to sell their goods in, there had to be a unique registration.

In broader terms, the new system changes and improvements include:

- Direct online registration for online sellers – marketplaces, e-commerce's and platforms – to a single EU Member State, that enables to pay VAT on all sales within the EU.
- New threshold of 10.000 EUR for distance sales of goods within the EU, that enables to sales below this limit to remain subject to VAT in the Member State where the taxable person is established;
- New rules for online platforms that facilitate the supply of goods;
- New record keeping requirements;
- Vat exemptions that were previously in place for small consignments – up to 22 EUR – were removed;
- The creation of the Import One Stop Shop to simplify the declaration and payment of VAT for all online sales up to 150 EUR, with special arrangements put in place for imported goods;

[48] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32017L2455

The one-stop system came to effect starting July 1rst 2021 which means we are yet to see the long terms results that this directive will bring, but it overall seems a good step forward. EU projections hoped to heavily reduce costs particularly for SMEs, making it easier for all sorts of organization to sell online[49].

[49] Morrison and Foerster. (2018). EU Digital Market VAT Reform. San Francisco.

Directive on the European Electronic Communications Code (EECC) – 2018/1972

This directive touches many different aspects of the telecommunication sector, with several objectives, such as:

- *Promoting and investing in high capacity, high speed networks, notably 5G and fibre optics.* To achieve this, the EU promotes co-investment and wholesale-only network management albeit "fair, reasonable, and non-discriminatory[50]." The concept is to separate the new operators in different branches, essentially rolling back network access regulation under specific conditions. Co-investment includes all sorts of conditions, such as: risk sharing in the long run, shared ownership, financing, and purchase agreements. All networks, being of the co-investment kind or the wholesale-only kind, must comply with the EU competition law, to ensure their fairness.
- Improve competition in the sector and generally boost the EU market. Better access prices and regulation, particularly assuring that there is coverage for those cases when EU competition law enforcement is not sufficient to solve a perceived market failure. Specifically, network access regulation is limited to operators with strong market power, or SMP (significant market power): in fact, before any adoption, the proposal is now reviewed by not only the EU Commission, but also from BEREC – Body of European Regulators for Electronic Communications), where is evaluated the chance of these proposals to change the trade power values and play among Member States. Furthermore, what is considered by many the most invasive form of access regulation, *cost-oriented network access pricing regulation* to wholesale markets, is limited to ensure better fairness and stability. This does also include Internet services: this concept is relatively new and for this reason it has taken a while for EU law to add these to the whole telecommunication and electronic communication services spectrum. The EECC refers to these services naming them *number-independent intrapersonal communications services* (NI-ICS) different from the already existent *numbered-based*

[50] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972

interpersonal communication services." The EECC maintains a broad authorization scheme, which allows any operator to deliver services within the EU without requiring a separate license. The general authorization system requires that each operator does a self-assessment and complies with all the applicable regulations of the relative telecommunication law. Finally, there is also the point of radio spectrum management point. The EECC establishes a more coordinated approach to spectrum management in order to promote 5G deployment and safeguard network investment incentives. The EECC makes the following improvements as part of this integrated approach: radio spectrum licenses for wireless broadband should be valid for at least 20 years to give legal stability and encourage long-term investments; a periodical assessment of radio spectrum fees; clear procedures for spectrum assignment and renewal.

- Protect consumers with better security, costs, and services: capped prices for calls inside the EU, better security of networks and services, protection in case of emergency situations, the establishment of a universal service for broadband and telecommunication that is both available to everybody and affordable, providing better transparency as well.

  The directive has entered into force in December 2018 and Member States had two years to implement it, with the deadline being put on December 2020. This is ensured not only among EU country, but to the whole EEA[51].

[51] Squire Patton Boggs. (2019). *The EU Electronic Communications Code.* London: Squire Patton Boggs.

Directive on the combatting of fraud and counterfeiting of non-cash means of payment – 2019/713[52]

This directive specifically targets fraud and counterfeiting of non-cash means of payment, harmonizing A revision of the Framework Decision (2001/413/JHA) was seen as particularly important in order to modernize the EU's reaction to new technologies including payment instruments that in a way can help businesses and consumers, but are reported to increasingly help criminal activities. This piece of law is also considered alongside the EU's efforts to improve cybersecurity, categorizing the new and updated elements of that make up illicit activities:

- Fraudulent use of non-cash payment instruments;
- Offences related to the fraudulent use of corporal non-cash payment instruments;
- Offences related to fraudulent use of non-corporal non-cash payment instruments;
- Fraud related to information systems;
- Tools used to commit offences.

An example of the value of this type of legislation is related to the misuse of contactless payment cards via RFI as explained by Klimek[53]: the European Union Member States must ensure that the following behaviour is punishable as a criminal offence when committed intentionally, according to Directive (EU) 2019/713 article 3 “the fraudulent use of a stolen or otherwise unlawfully appropriated or obtained non-cash payment instrument”. In this specific case, because an alleged criminal physical does not hold the contactless card, the offender, on a legal note, does not utilize it with his hands hence he does not operate it. However, he transmits an encryption key to the card using a false RFID reader, the card decrypts the encryption key, allowing all future communication to be encrypted using that key. The card reader sends the proposed transaction to the card, and the card "signs" the transaction. On the one hand,

[52] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0713
[53] Klimek, L. (2020). Misuse of Contactless Payment Cards with Radio-Frequency Identification. Masaryk University Journal of Law and Technology, 260-272.

contactless payments are limited to a narrow range of 1 to 5 centimetres when used regularly (or more). Fake RFID readers, on the other hand, can operate across a greater distance, such as a few meters.

In terms of liability, the Directive (EU) 2019/713 defines both natural and legal persons' criminal liability. Indeed, the Directive considers criminal culpability for corporations. However, it is debatable whether legal persons would be interested in such a criminal offense. It should be emphasized that criminal liability of legal persons for offenses has been a topic on the European Union's political agenda that has come and gone. Moreover, the Directive rules on all sorts of other possible issues:

- Jurisdiction and conflicts of jurisdiction;
- Investigative tools to effectively investigate fraud and the counterfeiting of non-cash means of payments;
- Exchange of information by national points of contact that are available 24/7;
- Establishment of channels that facilitate reporting of the offences described in the Directive;
- Encouragement for financial institutions and other legal persons to report suspected fraud or counterfeiting to law enforcement authorities.

In fact, the Directive further improves victim help and support, including provisions established primarily by the European Parliament throughout the deliberations. It extends the rights of victims within Directive 2012/29 to the unique demands of fraud victims who have used non-cash payment methods. In this regard, the Directive requires Member States to guarantee that natural and legal persons have access to specific information and assistance on how to protect themselves from the negative repercussions of the offenses, such as reputational damage. There is also a list of dedicated institutions that deal with various parts of identity-related crime and victim care. Furthermore, Member States are expected to promote single, national web-based

tools to make it easier for victims whose personal data has been exploited to get help and support[54].

[54] Wahl, T. (2019). New Directive Criminalises Fraud and Counterfeiting of Non-Cash Means of Payment. eucrim.

2.4 Key Regulations

General Data Protection Regulation (GDPR) – 2016/679[55]

The General Data Protection Regulation (GDPR) is the world's most stringent privacy and security law. Despite the fact that it was designed and passed by the European Union, it imposes duties on organizations anywhere where information or data about EU citizens is collected. On May 25, 2018, the regulation went into effect and those who break the GDPR's privacy and security regulations have to face severe fines, with penalties ranging in the tens of millions of euros. This law really showed a strong and forward step towards privacy and security over the Internet and telecommunication services, under the realization that people is putting their personal data in the hands of private organizations that operate in the web world every day: the general importance of this law for this thesis will require an in-depth explanation of several different aspects of this law.

The EU recognized the necessity for updated protections as technology advanced and the Internet was developed: as a result, in 1995, it passed the European Data Protection Directive, which established minimum data privacy and security criteria on which each member state's implementing legislation was based. However, the Internet was already transforming into the data Monster it is today with the first type of advertising emerging on the Internet already in 1994 and the majority of financial institutions offering online banking from the year 2000. Facebook became available to the general public in 2006 and a Google user sued the corporation in 2011 after the firm allegedly scanned her emails. Two months later, the European Commission's data protection authority determined that the EU required "a comprehensive approach to personal data protection," and work on updating the 1995 directive began. The GDPR went into effect in 2016 after being approved by the European Parliament, and all firms were expected to comply by May 25, 2018[56].

First of all, the legislation defined some key terms and actors that are essential to understand the stakes at play and the scope of the piece of law:

[55] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[56] https://gdpr.eu/what-is-gdpr/?cn-reloaded=1

- *Personal Data*. Personal data is any information that can be used to identify an individual, either directly or indirectly. Personal information such as names and email addresses is obvious, but not comprehensive. Personal data can include things like location, race, gender, biometric data, religious beliefs, web cookies, and political viewpoints. Moreover, online IDs and nicknames can also be considered part of this set of data, particularly if they clearly resemble the actual names of the actor.

• *Data processing*. Any action performed on data, whether automatic or manual, is referred to as data processing. Collecting, recording, arranging, organising, storing, using, deleting etc. with virtually anything being mentioned in the text of the GDPR.
• *Data subject*. The individual whose data is being processed is known as the data subject. These are your site visitors or customers.
• *Data controller*. This refers to the person who decides why and how personal data will be processed.
• *Data processor*. A third party that processes personal data on behalf of a data controller is known as a data processor.

We will now go over some of the most important and essential points that the regulation touches, which are data protection principles, accountability, security, design, allowance, consent, DPOs and people's privacy rights.

First of all, any data processor must practice according to seven principles related to protection and accountability that are outlined in Article 5.1-2. We are going to sum them up for easier comprehension on the following table[57].

[57] G. Kondova, J. E. (2020). Self-Sovereign Identity on Public Blockchains and the GDPR. CM SAC Conference, (pp. 342 - 345). Brno.

• *Lawfulness, fairness, and transparency*: Processing must be lawful, fair, and transparent to the data subject.
• *Purpose limitation*: Organizations must process data for the legitimate purposes specified explicitly to the data subject when they collected it.
• *Data minimization*: One should collect and process only as much data as absolutely necessary for the purposes specified.
• *Accuracy*: One must keep personal data accurate and up to date.
• *Storage limitation*: One may only keep personally identifying information for as long as it is required for the intended purpose.
• *Integrity and confidentiality*: Processing must be carried out with the utmost security, integrity, and confidentiality by using the relative and specific tools such as encryption.
• *Accountability*: It is the responsibility of the data controller to demonstrate GDPR compliance with all of the aforementioned criteria.

Secondly, data controllers must be able to demonstrate that they are GDPR compliant, according to the GDPR. And this is not something one can do after the fact: if one claims to be GDPR compliant but can't demonstrate it, then legal action will be taken. Organizations are suggested to take action to ensure excellent accountability and relative alignment with GDPR directives, such as assigning data protection roles to staff, keep precise and complete records of all the data gathered, how it is utilized, where it is kept, who's in charge of it and so on. At the same time, one must implement technical and organizational security measures after training the employees, and generally considering hiring third parties professionals to process data and take care of the issue. Finally, a Data Protection Officer (DPO) can be appointed for further help and to ensure compliance.

DPOs are required in specific cases related to companies that are heavily involved with data such as big tech companies like Google, Meta or Apple, or for ones that are dealing with criminal activity records or information, as well as public administrations and authorities. The EU recommends hiring someone on this role in any case, underlining the importance of understanding the GDPR rules and regulations and how

they apply to a certain company, instructing employees on their responsibilities, conducting data protection trainings, performing audits and monitoring GDPR compliance, and acting as a liaison with authorities. All tasks that are particularly important nowadays.

There are technical safeguards that have to be employed and organizational rules and methods that may be adopted to protect data from criminal or illicit activity: mandating two-factor authentication on accounts that store personal data to partnering with cloud providers that use end-to-end encryption; staff trainings, establishing a data privacy policy to any companies employee handbook, and/or limiting access to personal data to only those employees who require it; in case of data breach, the immediate notification to data subjects within 72 hours risking heavy fines. This is done to always ensure data security[58].

There's more to it: article 6 specifies when it is permissible to process personal data. Without having one of the following necessities or reasons it is impossible to collect, store or sell personal data. These include:

- An explicit and unequivocal consent to process the data from the data subject;
- Processing is required in order to carry out or prepare for the performance of a contract to which the data subject is a party;
- Legal responsibilities and obligations;
- Extreme cases related to security or life-threatening issues;
- Processing is required to complete a public-interest assignment or to carry out an official function.

In terms of consent, firmer rules have been applied from a data subject perspective, with several points being raised such as:

[58] Savić, D. &. (2018). Challenges of General Data Protection Regulation (GDPR). *Sinteza 2018* (pp. 23-30). Beograd: Singidunum University.

- Freely provided, precise, informed, and unambiguous consent is required;
- Consent requests must be clearly distinguished from other concerns and written in clear and simple language;
- Data subjects have the right to withdraw previously given consent at any time, and you organization are forced to respect the choice of the subject.
- Children under the age of 13 can only offer consent with their parent's permission.
- Evidence of the consent must always be clear and transparent.

Finally, there's a dive into the privacy rights of individuals, that got empowered by the GDPR: the goal of these rights is to offer people more control over the data they loan to businesses. It's critical for companies to understand these rights in order to comply with GDPR and put their values always at the centre of any data related decision. The following is a list of the privacy rights of data subjects:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling[59].

[59] Daniel Mikkelsen, H. S.-J. (n.d.). *GDPR compliance since May 2018: A continuing challenge.* McKinsey & Company.

Roaming implementation regulation – 2016/2286[60]

A concept that is more related to regular telecommunication in general, roaming has quickly become more and more important the more mobile Internet connection became popular among users. Roaming charges, for the most part, are defined as the additional costs that a telephone company applies for calls, messages, Internet connection and general service use outside the original country in which the user signed the contract.

The European Commission raised the issue of high roaming charges among different Member States multiple times and when high roaming charge prices still remained in 2006, the Commission considered intervening in the market by establishing maximum rates that mobile network carriers had to charge to their subscribers and that could not be surpassed. The European Parliament and the Council of Ministers both approved the proposed regulation, which became legislation in June 2007. Retail and wholesale voice roaming charges were to be capped as of August 30, 2007, unless a special roaming tariff was in place. In 2008 and 2009, the maximum costs were set to drop even more. Customers traveling to another member state were also expected to get a text message informing them of the roaming charges that apply[61]. Initially, the price caps were only in place for a limited time, and they were set to expire on June 30th, 2010. The 2007 regulation's deadline was pushed out to June 30, 2012, and it was expanded to include text messaging and data roaming. It also included annual price decreases until the regulation expired, as well as mandatory per-second billing after 30 seconds for calls made and per-second billing throughout for calls received.

The EU updated the regulation in 2012 after concluding that market conditions did not support reducing the roaming cap within the EEA. Retail roaming capping rates expired in 2017 under the 2012 rule, and wholesale roaming capping prices are set to expire in 2022[62].

[60] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R2286
[61] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:171:0032:0040:EN:PDF
[62] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:172:0010:0035:EN:PDF

Thanks to this regulation, retail roaming charges effectively got removed, and from June 2017 mobile users that travel in the EU are able to access their own tariff even when travelling abroad in the EU.

The Regulation on cross border portability of online content services in the internal market - 2017/1128[63]

The Portability Regulation prevents geo-blocking – essentially a block on content based on location - of online material within the European Union as of April 1, 2018. The rule governs all European citizens' unfettered access to paid subscription Internet content, services, or products, regardless of their location within EU territory. Providers of fee-based online content are thus required by this regulation to provide cross-border portability to its subscribers with no. It is not permitted to restrict access or charge additional costs. This particular regulation on portability does not apply to offerings that are not directly responsible to payment, such as media libraries. These services are provided on a purely voluntary basis. Finally, just like the whole DSM package, the portability regulation aims at limiting the amount of personal data gathered from users, to improve transparency.

Before the adoption of this regulation, a number of obstacles made it hard for consumers to access their paid services, particularly copyright and anti-trust laws: these are, in fact, regularly granted on a territorial basis – movies, music, tv series etc. – making it impossible for providers to extend portability to different countries without a ad-hoc legislation that enables it. To strike a balance between competing interest, the regulation, on one side, provides users with access across all EU, with the privilege only available to users who are based in the EU, not to those who only pass through temporarily, and on the flip side, it attempts to maintain solid the rights and interests of copyright owners[64].

[63] https://eur-lex.europa.eu/eli/reg/2017/1128/oj

[64] Sebastian Engels, J. B. (2017). The Portability Regulation (Regulation (EU) 2017/1128): A Commentary on the Scope and Application. Journal of Intellectual Property, Information Technology and E-Commerce Law.

The regulation on the promotion of Internet connectivity in local Communities - 2017/1953[65]

Informally known as the WIFI4EU policy, this regulation aims at providing free and unlimited Wi-Fi access to public areas all over the European Union. Compared to the others, this regulation is quite straight forward: a voucher of 15.000 EUR is provided to municipalities that register in the provided online platform during specific calls. WiFi4EU provides money that can be spent to cover installation and equipment costs related to the Wi-Fi hotspots – wireless access points - and needed tools, while public administrations are still required to pay for the Internet subscription and the maintenance of the aforementioned equipment.

The requirement is that at least 3 years of free and high-quality Wi-Fi connectivity must be provided to the public, in selected "centres of public life" and the voucher could also have been spent towards a bigger project related to digitalization.

[65] https://eur-lex.europa.eu/eli/reg/2017/1953/oj

Geo-blocking Regulation – 2018/302[66]

This regulation tackled the issue of geo-blocking, which can be described as the restriction to the access to online content relative to the location of the user. To favour the Digital Single Market, the Commission ruled against this discrimination, targeting e-commerce and online shops selling goods inside the EU landscape that often would refuse to sell particular goods or services in other countries, effectively discriminating certain countries because of unfavourable national policies, VATs or costs. Contrary to popular belief, it is not mandatory for these stores to deliver goods to every single country if they don't want to, but if they do so, it must be possible to buy those services or items at the same conditions of the ones of the country of origin.

To better understand the key rules, customers must be allowed to:

- Access and browse every online store, e-commerce, or service vendor without restrictions, and must be asked permission when a system of auto-redirection is put in place.
- Despite the nationality, country of residence or establishment, a user always must be allowed to shop for goods or services in any EU website: this extends to regular people, and also in B2B – Business to Business – sales for personal use of the company.
- Rights must be equal among different countries: as explained before, the same conditions – and thus prices - have to be applied to all transactions without differences among all EU citizens.
- To access all different methods of payment – again, without discrimination of any sort – with exceptions only in case of suspected fraud, cases upon which the seller can ask for different and more advanced forms of payment.

At the same time, the rules that apply to online sellers and traders are the following:

- E-commerce must sell their goods and services to all EU customers without exceptions, offering the same conditions despite nationality, residence, or establishment.

[66] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018R0302

- Traders are not obliged to deliver outside their chosen delivery area, being transparent on to which countries they offer delivery to and to which ones they don't.
- Even if prices must be the same for any citizen, stores can charge different prices in different sales channels and countries, with the VAT being paid in the country that accommodated the initial delivery. Prices cannot be changed based on the IP address or location of the user though, so this just applies to a single website. For instance, Amazon has different websites for each country (Amazon.it / Amazon.de / Amazon.fr etc) in which it can set whatever price it wants. Despite this, an Italian citizen that wants to buy a certain product from Italy but on Amazon.de will be able to do it exactly the same way as a German would be allowed to, paying German VAT.
- Traders can offer whatever payment method they want, and, again, are unable to discriminate by location.
- Since different countries in the EU have different rules that allow certain products or services, in terms of safety, chemical composition or labelling, it is a duty of the customers to ensure that the product is legal in their country of residence. It is not mandatory for stores to inform customers about this[67].

67 https://www.eurocommerce.eu/media/155816/eurocommerce_faq_on_the_implementation_of_the_geoblocking_regulation_readonly.pdf

Cross border parcel delivery Regulation - 2018/644[68]

This specific regulation targets delivery services that use shady or simply different pricings in cross-border shipping of goods, pursuing transparency and equality among Member States. Transporters are required to publish and make available on their personal website the costs of parcels in the country of origin and in all other European Union member states.

Moreover, a regulatory oversight is put into place to better control along with a database named PARCEL, launched in April 2019, that collects data and it is updated each April with parcel tariffs, with products being defined in the annex of the Cross-border Parcel regulation.

[68] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32018R0644

The single Digital Gateway regulation - 2018/1724[69]

From 2020, citizens and organizations that want to move freely inside the European Single Market, can do so by using the Your Europe portal, effectively a Single Digital Gateway on all existing rules on a national and European level on all sorts of useful matters, such as business, work, education, and taxation. The main objective of the regulation is to grant a common access to quality and selected information, along with tools to assist citizens and organizations.

The Single Digital Gateway provides access to:

- Information related to rights, duties and European and national regulation that applies to all those users that want to enter or operate in the European market.
- Information on procedures online or offline, and links to online procedures, established at the national or European level, to allow citizens and organizations to operate freely and inside the boundaries of the law inside the EU market framework.
- Information of how to get assistance, particularly to access towards the services that are more suitable the user, and until 2023, also access to the management of more than 20 administrative documents and procedures, such as birth certificates, VAT reports and university papers.

[69] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1724

The Regulation on the free flow of non-personal data in the EU - 2018/1807[70]

This regulation went a bit under the radar compared to its close relative, the GDPR, which we thoroughly described earlier, but it stands as one of the most important regulations for companies that work with data, particularly in newer and upcoming applications such as IoT, AI, Deep and Machine Learning and generally the industry 4.0. This relates to non-personal data, which can be defined as web-based information that cannot be linked to a user or a natural person. The thought behind this regulation is that the only way for a value chain to work effectively and efficiently is to make the process of information travel as smooth as possible: to do so, two fundamental obstacles must be dealt with.

- Member states have their own data localization requirements, making it hard to comply to every single rule of each and every country in the EU framework. Data localisation requirements, or the responsibilities placed by EU members on firms to locate data centres in the national territory of a particular Member State and to process it locally, are one of the primary issues addressed by the regulation: in fact, these requirements hinder growth by making it harder to create a ecosystem of data technologies that can effectively by cross-border. Moreover, companies are forced to have multiple IT infrastructures for each Member State in which they operate data in, making the whole operation way less straight forward and money efficient. This in turn, makes the European big data market less competitive, which in times of great technological change and growth in this direction, is particularly penalizing for the whole European digital economy.

- Vendor lock-in practices: customers that are reliant on a single cloud provider's technology and are unable to move vendors without incurring in significant fees, legal restrictions, or technological incompatibilities. This hurst competition. To solve this, the regulation makes it easier for firms to create self-regulatory codes – mind the fact that there's not a new regulatory

[70] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807

> requirement of any sort, it's just self-regulation – that work under the principles of openness, interoperability and open standards.

Fixing these two issues would, in the mind of the legislator, remove the major roadblocks and enhance the data economy by promoting cross-border data sharing, allowing corporations to store non personal data wherever they want as long as its inside the EU borders. At the same time, authorities will not be prevented from accessing data just because it is processed in a different country, because the regulation does not affect competent authorities' powers to request and obtain data required to solve national or European legal disputes.

A final remark regards the connection between this regulation and the GDPR: in this context the term "mixed datasets" is used to describe those sets made from personal and non-personal data. In these particular instances, the regulation applies just to the non-personal part of the set, but in those cases when it is impossible to decouple the two kinds of data, the GDPR is the law of reference. This means that, from a compliance point of view, companies had to deal with a detailed examination of all the data, having a firm regulatory distinction between the personal and non-personal data, with the latter being sometimes considered non-significant.

Body of European Regulators for Electronic Communications (BEREC) Regulation - 2018/1971

This regulation established BEREC. BEREC is a consultative body aimed at improving the Europe Telecom market: the body publishes guidelines, opinions, and directives related to the telecommunications market, and it is responsible for reporting on the more technical issues. According to their 2021 report, BEREC: "aims at fostering the independent, consistent and high-quality regulation of digital markets for the benefit of Europe and its citizens." The general goal of the regulation is to increase competition in the European telecommunications market and protect the EU Bring citizens to market and enable new technologies like 5G71.

The 2022 work programme includes 3 strategic priorities that aim at helping EU population and member states to get more connected:

- *Promoting full connectivity*. Promoting comprehensive connectivity has been remarked as one of the main strategic priorities for the next five years BEREC, aligning with the renewed focus on rolling out ultra-high-capacity networks inside the European regulatory framework. This means prioritizing and improving the tools for expansion of safe, competitive, and reliable high-performance networks (in both fixed and wireless form) across Europe while transitioning smoothly from the existing legacy infrastructure. This appears extremely important in the light of the data we analysed regarding 5G and high-capacity network distribution in the EU: having a dedicated actor that ensures this is a good step to ensure results. More in detail, this actor is working on migrating from copper-based connection to faster fibre optics links, that, like we have previously mentioned, is necessary to achieve high bandwidth connection in all areas of the Union. In order to make it simpler to achieve goals such as this, BEREC uses the report as a tool – the one in question being named "BEREC Report on a consistent approach to migration and copper switch-off."

[71] BEREC. (2020). BEREC Work Programme 2021.

Other reports include, the "BEREC Report on regulatory treatment for backhaul" that aims at creating the backhaul necessary to enable 5G and high-speed connections to be deployed in less populated areas. To clarify, for backhaul we mean the necessary portion of the network that links the backbone network and the small subnetworks closer to the end users.

- *Thriving sustainable and open digital markets.* Promoting work related to the operation of digital markets, with a particular emphasis on examining and assessing the conditions and concerns relating to digital service providers and users is one of the core points of BEREC's strategy for 2022 and onwards. Understanding future developments quickly and analysing upcoming technologies such as cloud-based solutions, AI or big Data can help to prevent the same enterprises taking over the market (like it's already happening). Moreover, BEREC aims to help spreading 5G in a healthy and safe way, by ensuring a consistent framework that cannot be exploited by just a few companies or groups of stakeholders.

- *Empowering end-users.* The final point regards end-users: getting everybody onboard with the rapidly changing technology world is hard, but absolutely crucial to level the plain field and ensure that the average consumer is aware and protected when, inevitably, he/she will get in touch with Internet services. To achieve awareness and good interactions, BEREC is pursuing high quality connection that can give the basic tool to empower the user and make life easier.

The regulation on ENISA - 2019/881[72]

This regulation targets cybersecurity, namely by establishing a new framework for European Cybersecurity Certificates and strengthening EU cybersecurity agency's mandate. The EU Cybersecurity Certification Framework is an internal market measure that establishes the basic horizontal requirements for developing schemes related to certification in cybersecurity matter inside the European Union. All products related to the Internet, as well as services and processes must be certified, in accordance to specific security measures to ensure the ultimate protection of the authenticity, availability, integrity and confidentiality of data that has been stored, transmitted or processed.

This regulation aimed at improving online security for all the following actors in different ways:

- Citizens/end users: by working to ensure better online security, the trust towards more efficient, digital technologies would improve, and regular people would feel less danger handling their mobile daily and accessing online services.
- Service providers, online traders, and web-based organizations: thanks to a one-time certification system, companies are not only able to get through the certification process just once, but they also get hold of a stronger certification, valid inside all the European Union. Moreover, the fact that these products/services are deemed cyber secure by a certified authority, makes the items more compelling to customers inside the market.
- Governments: better information on products and services in case of state expenses on ICT products and services.

The new EU framework establishes voluntary certification schemes, which means that vendors and providers can independently chose to get their products certified or not, with the chance to make this mandatory in the future.

[72] https://eur-lex.europa.eu/eli/reg/2019/881/oj

The regulation also transformed ENISA's temporary mission into a permanent one. The agency strengthens by receiving additional personnel and funding to help carry out important tasks such as:

- Cybersecurity legislation development and implementation.
- Capacity building and improvement.
- Encouraging collaboration and coordination on cybersecurity issues.
- Becoming an autonomous cybersecurity expertise centre.

Platform to Business Regulation - 2019/1150[73]

This regulation aims at tackling the issue of intermediation, third-party online platforms: the EU recognized that businesses that expand online heavily rely on these types of services, making it important to regulate the relationship between businesses and mediation platforms, to ensure transparency and to avoid the aforementioned platforms to achieve too strong of a position in the market.

To achieve this, the regulation establishes clear rules that must be followed by platforms and makes it easier for business to comply and to know if a platform is operating under the rules of law. Breaches of the terms will lead to the nullity of the obligations, making it again easier for businesses to defend from fraud without years of lawsuits. Moreover, platforms must adhere to specific requirements when restricting, suspending, or terminating their services, publishing an accurate statement with clear reasons to explain the decision, at least 30 days in advance if it's the case of platform service termination. Furthermore, platforms are required to have an internal structured in place to handle discussions and complaints with the businesses they deal with, in order to ensure better transparency and ease of service.

Platforms must disclose information about the primary characteristics of the algorithms used to rank all the different products listings, and why they prioritize some or others, clarifying if customers can or cannot influence these rankings both directly or indirectly. Obligations also include data transparency, that again is at the centre of the regulation under the framework of the Digital Single Market, specifically in this case ensuring that platforms are clear about data usage. It was in fact common that companies shared data with other companies with just market purposes instead of development purposes. This is no longer possible thanks to this regulation, that enables companies to decide whether or not to share data, depending on the intended uses that the platform has to clearly state74.

[73] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R1150
[74]https://www.osborneclarke.com/insights/regulation-eu-20191150-new-rules-protect-business-users-online-intermediation-platforms

3. EU Digital Policy: issues and possible solutions

April 28th, 2022 was an important day for the future of the Internet worldwide: in this day, the European Union and the United States, along with many international partners, have proposed a Declaration for the Future of the Internet, to state the vision and the mission for the Internet ecosystem in the years to come[75]. The vision, though, appears not to be that different from the one that was already established with the Digital Single Market. Going over the pillars of the Declaration, it is clear that the growth was slower than expected:

- Protecting human rights and fundamental freedoms while accessing online services, to make the Internet a less dangerous and exploitable environment.
- A more global Internet, expanding access to users living in remote areas.
- Inclusive and affordable access to the Internet, lowering prices and helping families in need giving free access.
- Developing trust in the digital ecosystem, with clear regulation towards e-commerce and service providers, while being more transparent to citizens regarding decisions that affect them.
- Create a multistakeholder Internet governance, to make it a more competitive, fair and safe environment.

Of course, this declaration is a declaration of intents between different institutions of different countries in the world, and thus it is understandable that the values are similar to the ones pursued by the EU in its own internal policies. Covid surely played a role in slowing down the process of ICT development, particularly in developing countries[76].

But at the same time, it appears that the issues that were present in 2014 when the Juncker Commission was elected, are still relevant today.

Transparency, trust, a worldwide high-speed connection for everybody, security and regulation towards tech giants that work with data are problems that the EU was not

[75] https://digital-strategy.ec.europa.eu/en/library/declaration-future-internet
[76] https://sdgpulse.unctad.org/ict-development/

able to completely solve in the last few years. There are several reasons for this and the first is clear after our previous analysis: with new technologies being piloted every day, the EU just cannot keep up. Being the digital world so multi-faceted, the actors and stakeholders involved are a lot: supranational political actors, national actors, and companies as well as interest groups, leading to everlasting discussions that often result in halfway decisions that do not tackle the issue at stake. Moreover, being such a profitable and new market, there is a great number of companies that have more knowledge and power compared to every other market. These companies are able to get inside the EU institutions, pushing interests and forcing their own narration of new technologies, making it even harder for the institutions to understand what is at stake.

To further analyse this point, where going to use as an example probably the clearest instance of political discussion and challenge of the last few years, one that touches all the main points that we've made when discussing the direction and possible issues of the EU in terms of Internet Policy: the regulation of online platforms and service providers (DSA).

3.1 Study case: Digital Service Act (DSA) and Digital Markets Act (DMA)

The Digital Service Act and the Digital Markets Act are the latest policy related to the digital economy in the European Union, aimed at making the digital space safer and protecting the fundamental rights of users and at creating an environment that fosters innovation, growth, and competitiveness[77]. Even if an agreement was reached in March 2022 on the DMA, and the DSA was set to be agreed upon on late April 2022, Big Tech companies pushed a strong, last-minute attempt to push their interests into the decision-making process. The main interest of the Big Tech companies such as Google, Apple, and Meta, was to cancel or tame the regulation regarding the limitation of surveillance advertisement, as well as increasing the leverage in the market to maintain their position of power over smaller competitors that are encouraged by the EU to enter the market, to foster competition. This push was exposed by the release of documents by the Corporate EU observatory[78]. A report by Corporate Europe helped us put together all the relevant information about the topic[79].

The aforementioned proposals might have a substantial impact on how tech behemoths like Google and Apple conduct business and make money, as well as address some important public interest issues relating to people's online lives. The tech industry titans didn't take this danger lightly; they exerted significant pressure on the EU Commission during the formulation of the proposals before moving on to the Council and Parliament already in the 2020 period.

All big tech companies, as previously shown upped their expenditure on EU lobbying over this time, according to new self-declared lobby data through the not so reliable transparency register. In just one year, the Big Tech companies collectively spent more than 27 million euros. All five businesses increased their lobbying spending, but Apple had the greatest jump, nearly doubling their outlay (see Figure 15).

[77] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
[78] https://handlingar.se/en/request/digital_services_act_digital_mar_2#incoming-2249
[79] https://corporateeurope.org/en/2022/04/big-techs-last-minute-attempt-tame-eu-tech-rules

These companies turned their attention to the trilogues, the final step in the development of EU policy, in which the Council and the Parliament attempt to reach a consensus while the Commission serves as the mediator: during this phase, just a small number of negotiators is present, the rapporteur responsible, the minister in charge and the responsible commissioner. Between 70 and 80 percent of the European Union's legislative acts were approved after a trilogue in 2018, according to the EU Parliament. The final trilogue agreements were often immediately adopted.

This process, which is held totally behind closed doors and with almost no public access to the debates, is one of the most hidden phases of EU policymaking and access to materials pertaining to these conversations is typically not permitted. The EU Institutions have stated that part of the reason for this confidentiality is to stop pressure from lobbyists on the decision-makers, but despite this, it stands clear from the information that emerged that active corporate lobbying has been pushing interests nonetheless, even in trilogues, by using heavy expertise to make matters even more technical, in the attempt to create loopholes and set the stage for later developments that the EU is not aware about. This was done by meeting with commissioners, completely off the record, accessing restricted information without consequence[80].

Discussions of the Digital Services Act and the Digital Markets Act were dominated by surveillance advertising: the recommendations made by the European Parliament to outlaw or at least severely restrict advertising were effectively thwarted by a strong corporate backlash. In a last-minute surprise, the European Parliament approved new restrictions on surveillance advertising, including a ban on targeting children and the use of collected or implied sensitive categories of information (such as religion, sexual orientation, race or ethnic origin) to target vulnerable individuals.

While noting that it still isn't enough, civil society organizations applauded this progress. Banning advertisements that monitor children or that are based on sensitive

[80] EDRi. (2016). Response to the European Ombudsman's public consultation on the transparency of trilogues. Brussels: EDRi.

personal data is a very welcome step forward, but this won't stop pervasive online commercial surveillance, according to the EU consumer organization BEUC.

The great deal of data on people from sources like the websites they visit, their search engine lists, information on videos and media, the type of device they use, their geographic location, other apps they have downloaded, their purchasing history, etc. is the foundation of surveillance advertising, also known as tracking or behaviour advertising. A user profile is created by gathering data from a user's online activities, such as age, economic status, political leanings, religion, sexual orientation, physical and mental health, and other personal information, that can all be found in these profiles and can be easily observed or inferred. Following that, users are micro-targeted with advertisements using this data.

In recent years, criticism about surveillance advertisements has risen for multiple reasons, like the alleged violation of people's privacy and data protection due to the extensive data collecting – thus the term surveillance - that such advertising relies on. Additionally, prejudice, bias creation, deceptive political campaigns, and the exploitation of those in vulnerable situations have all been related to personalized marketing. Digging further into this case, we can see that Google lobbied heavily in different ways during 2021, particularly towards the European Commission:

- In November, Sundar Pichai, the CEO of Google, met with Margrethe Vestager, the executive vice-president of the EU Commission. The Commission's records about the meeting revealed that the Parliament's debate of a potential ban on surveillance advertising was one of his top worries.
- In December, Google again raised the matter with Vestager's cabinet addressing their worry about the newest draft in the IMCO [European Parliament Committee on the Internal Market and Consumer Protection] Committee in a direct response to the draft stance of the Parliament. The lead MEP's draft stance included a default opt-out from surveillance ads in the IMCO, which was the principal committee in charge of the DSA.

- In January 2022, Google lobbied national governments, producing a thorough analysis of the context and the proposal of the EP, the EC and the Council, to try and push national states towards its side: these actors, even if far from the EU institutions, can influence European decision making towards the Council. Moreover, the national territory is uncharted and unregulated, making it easy to make meetings without appearing in the register[81].
- In March 2022, a last push from Google tried to undermine the proposals regarding surveillance and bans towards minors: the company wanted to allow people to know the criteria they used to target them, but in a very restricted way, effectively not giving reliable and updated information to users[82].

It stands clear that Google has been heavily impacting decision making, even if the details are unclear, just like it seems unclear the way in which the EU aims at preventing these companies to influence from the inside the decision-making process.

This can be said also about other big tech giants in this particular policy case, notably Meta and Spotify: the former tried to influence the Swedish Ministry of infrastructure regarding marketing practices and the balance with transparency, the latter advocated towards the targeting of minors, particularly the limits imposed for registration and consumption of content from a particular online platform.

Regarding the brother of the DSA, the DMA, we also had strong lobbying with Apple leading the pack in terms of the push back practices they tried to impose on regulations that could have hurt their services. Apple general argument was that new regulation that undermined the independency of its platforms such as the Apple Store. There were two important moments in the lobbying push from Cupertino:

- In September 2021, Atlantic Council, a notable think-tank, had an off the record meeting with Commissioner for Justice Didier Reynders, to pursue

[81]https://corporateeurope.org/sites/default/files/2022-04/I2021_01055-66%20Overall%20Trialogue%20priorities%207854189_1_1_Google%2028%20feb.PDF
[82] https://corporateeurope.org/sites/default/files/2022-04/Minnesanteckningar%20Google%2022%20feb%202022%20en-GB.pdf

Apple's case on DMA and particularly on cybersecurity and there is no information regarding what was discussed.

- In January 2022, the first trilogue meeting was held regarding the DMA, with results that definitely didn't suit Apple's interests. A final attempt concerning the concept of side-loading and the extension of interoperability was made by interacting directly with the Swedish government, thanks to a paper on interoperability, that had an impact. In fact, the final text of the DMA[83] opened to a safeguard, that enables organizations to justify the non-compliance towards this particular rule.

What conclusions can we draw from this case study?

- Big Tech companies have a huge number of resources of any kind: knowledge, money, influence and so on. This enables them to get at the front of the queue when it comes to pushing interest into policy making.
- The EU does not have the right tools in place to defend from Big Tech companies: the revolving door issue, together with the lack of transparency on both the national and the European level makes it easy for organizations to push their interests forward, with common organizations such as NGOs struggling to keep the pace of the front runners. Notably, the transparency register is flawed with the lack of a mandatory registration of meetings, creating a lack of accountability, ethical behaviour, and honesty.

This example fully represents the landscape Internet related policy makers had to deal with for the past 15 years, and we can assume, thanks to our previous analysis, that even before the advent of the big service providers – the so-called Big Tech giants – we had the telecommunication monopolists imposing their knowledge and interests onto the regulators.

[83] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN

3.2 The 2022 EU agenda: policy, politics and lobbying

The whole ecosystem of the tech and telecom industry is now deeply intertwined thanks to the Internet: this creates constant and multiple debates that, even for an institution such as the EU, must take into consideration the interests of outside countries, companies, and organizations. The discussion of the future still resembles and touches many points that we have already crossed in our analysis: thanks to previous research and also by researching the most recent discussions among EU commissioners and representatives, we can make a few hypotheses on what the future holds in terms of tech, telecommunication and Internet discussion.

The first important point in the EU agenda is the lack of scale compared to the United States. Organizations, particularly service providers that deal with data, media of all kinds, and social media seem to all come from the U.S., and European firms struggle to cooperate and work together, as per a recent gathering on the topic that included various stakeholders, MEPs and Commissioners[84]. Telecom operators have to scale up, get together and become more active and influent in the market, to be relevant in the worldwide scenario of the new technologies, notably 5G, data and cloud services.

More global relevancy would enable for a better understanding of the market itself, thanks to the extra knowledge that would inevitably be produced, along with the economic value at all levels of having more competition.

As suggested by Jacobides (Jacobides, 2020), Europe could benefit from a well-regulated system, in harmony with the dominant countries in the market, specifically China and the US. This way it would be possible to protect and defend smaller companies and individuals that struggle internally because of external factors: the lack of consistent regulation though makes this hard to do. The idea would be to trail the moves of the leading pack, to catch onto new and thriving ecosystems and technologies that could take the EU back on top of the chain. To do this, a strong foundation has to be set, and even if the current regulations seem to be stacking up well to the current situation, there's still many challenges ahead.

[84] https://etno2021.live.ft.com/agenda/session/590008

Another key point is the paradox of regulation that has also emerged from the analysis we have made so far. To defend user's values and to protect them from all the possible risks of the web, a strong regulatory framework has been established in the past 15 years by the European Union. This happened in all related fields, such as privacy, data protection and user identity. In fact, the aim of the EU has been "net neutrality" for some time now: net neutrality is described as the principle that each and every Internet data package, despite its content, destination, origin etc. should be treated the same way every time[85]. The fact that companies such as modern service providers can limit access to certain data makes it for a difficult ethical discussion that has been at the core of the political play in the EU and the U.S regulatory playfields for quite some time[86].

To make things even more complex, there are two sides in the market, the ISP side, and the content provider side: potentially, the first, related to ISP such as TIM, Vodafone or AT&T in the U.S., companies that provide the physical connection to the broadband, can discriminate content providers based on interest. Moreover, users can be discriminated from both, content and service providers. This is why the regulatory framework quickly tried to achieve neutrality in the EU creating BEREC, the Body of European Regulators for Economic Communication, that we have already analysed and that aimed exactly at prohibiting prioritization practices (BEREC, 2020). At the same time, the United States pursued a similar strategy as shown in Figure 16.

[85] S. Greenstein, M. P. (2016). Net neutrality: a fast lane to understanding the trade-offs. *American Economic Association*, pp. 127-150.

[86] Garcia, L. K. (2021). John Rawls and the limits of net neutrality in the Internet market: new ethical insights for entrepreneurs. Filosofía y Ciencias Sociales En Tiempos De Desconciert, 1190-1205.

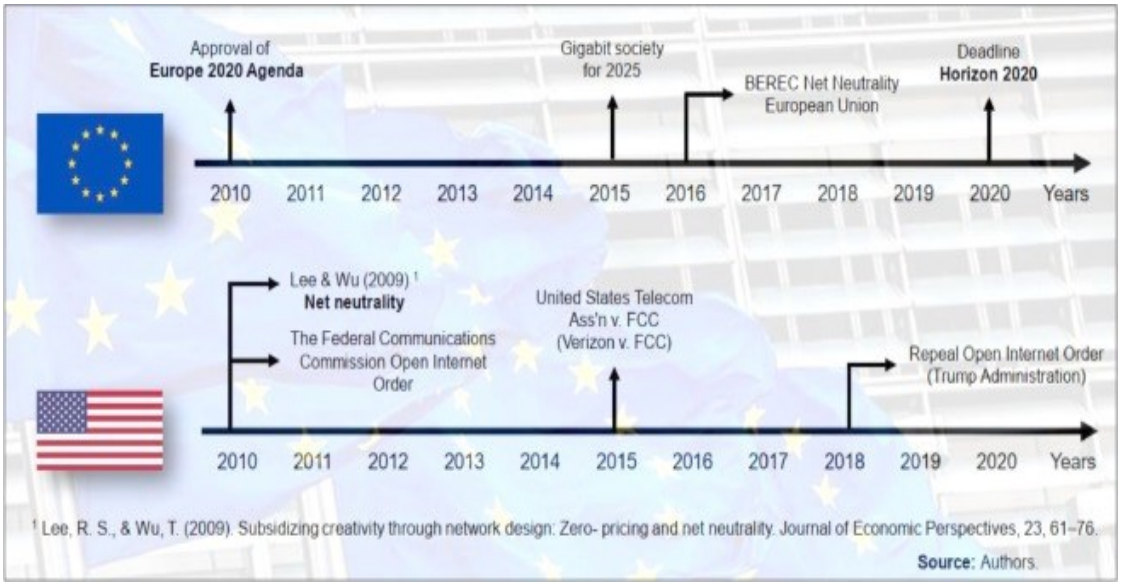

Figure 16. How Internet regulation evolved in the EU and in the US

The current political situation sees ISPs go against Big Tech when discussing net neutrality: Big Tech is the idea that innovation can only be achieve by freedom and neutrality, creating the most open and global Internet as possible. On the other hand, the argument of ISPs is that net neutrality regulation was working well in the 1990s when it was less strict and enabled for more private investments to increase broadband capacity and speed. With the current regulation, ISPs fear that investment is not fostered enough, making ISPs work much more like public utilities and much less like fast growing companies.

The debate has been strong, but the ISP position has not been very popular in the European Commission's halls: the balance has been in favour of Big Tech companies for quite some time, because of lobbying but also because openness is a shared value among the EU and Big Tech[87]. In fact, since the first instances of discussion, the market has changed quite a bit, and service providers became way less relevant, with content providers becoming more and more resourceful and overall important in the market and in the political discussion. The issue now comes more from the fact that Big Tech has

[87] T.W. Hazlett, J. W. (2017). The Effect of Regulation on Broadband Markets: Evaluating the Empirical Evidence in the FCC's 2015 "Open Internet" Order. Springer - Review of Industrial Organization, 487–507.

risen to hights that enable themselves to discriminate: as a consequence, it is clear that the regulatory framework is not up to date to fight a new challenge, which appears to be way more nuanced that the one before[88]. The attempt, from the EU side, is to fix this with the aforementioned DSA and DMA, which are more updated pieces of regulation, an umbrella of policies that hopefully will balance out the power difference that now stands between Big Tech companies, users and ISPs.

But the political discussion does not involve just the net neutrality issue: what comes after the DSM is probably a more de-regulatory oriented path rather that one that imposes more and more regulation. Let's take the GDPR, the General Data Protection Regulation that we have thoroughly described earlier for example on this. Since its inception, the regulation has been criticized for being too complex. By having so many obligations, companies need to hire a data protection officer, making this problematic for the smaller companies that wish to enter the market with a limited number of resources. And there is more to this: according to a report by Ilse Heine, the fact that Member States are the ones to supervise the companies working inside its borders, makes it tough for the available resources: the issue of power that keeps coming up in this analysis is still coming up here as well, with legal teams from Tech Giants with unlimited resources constantly disputing fines and making it hard for the Irish authorities – where Tech Giants are established -. This is leading to even more tension, with the European Parliament discussing infringement procedures towards Ireland for not enforcing the rules of GDPR[89]. It stands clear that the so called "one stop shop" is not very reliable in the current context.

Geo-blocking has seen strong discussions itself, particularly from small business owners and aspiring e-commerce stores: the fact that delivery has to be ensured to every other country, can make it hard because of the different costs that each countries' rules enforce. Jacobides here argues that to remove borders is an effective way to create a strong open digital market, but at the same time making it mandatory to businesses to

[88] Jacobides, M. G. (2020). Regulating Big Tech in Europe: Why, so What, and How Understanding Their Business Models and Ecosystems Can Make a Difference. London: London Business School.

[89] https://www.euractiv.com/section/data-protection/news/european-parliament-calls-for-infringement-procedure-against-ireland/

ship to every single country seems to fundamentally hinder competitiveness more than it is able to foster it. Moreover, the political challenge that arose along with this regulation created a very compromised norm that does not resemble its original vision in many cases, with the regulation still being discussed with some willing to completely remove all barriers regarding geo-blocking practices[90].

Regarding VAT, the issue is clear, and impacts so many other policies, notably geo blocking: the fact that there is a number of different VAT rates across different Member States makes it difficult to manage costs for exporters, creating a much less favourable market to work in. Some research argues that the latest developments seem to lead towards a common 20% VAT rate across all countries, but harmonization seem still out of reach[91]. The work made withing the context of the DSM seems to be appreciated by all parts of the political discussion, but still a step has to be made in the opinion of the European Parliament itself, according to a recent report[92].

Regarding e-invoicing:

- "Promptly establishing a harmonized, common standard for e-invoicing across the EU, preferably in 2022. The aim is to reduce costs related to the creation of dissimilar and divided e-invoicing systems across the EU;
- Establishing the significance of real-time tax reporting and e-invoicing;
- Considering the gradual implementation of obligatory e-invoicing across all Member States by 2023".

Regarding reducing the VAT gap:

- "Directing attention to how the VAT gap is impacted by the exemption of cross-border Union trade;
- Establishing simpler measures to comply with VAT obligations;
- Receiving data for monitoring and addressing tax fraud;
- Using e-invoice data for fraud detection".

[90] https://www.europarl.europa.eu/news/en/agenda/briefing/2021-03-08/16/meps-expected-to-seek-an-end-to-remaining-geo-blocking-restrictions
[91] Feria, R. d. (2014). La Réorientation Européenne De La Tva À La Suite Du Renoncement Au Régime Définitif. Toulouse: Presses de l'Université Toulouse 1 Capitole, LGDJ - Lextenso Editions.
[92] https://www.pagero.com/news/european-parliament-vat-requirements/

Regarding the previously discussed roaming regulation, approved in 2017 but in the making since 2015, the political discussion has seen Euro sceptical parties, notably Ukip, arguing that telecom organizations would have raised domestic prices to make up for the loss of the high tariffs when abroad. Generally, this has shown not to be true, with companies resorting to other ways of making revenue such as new services or smartphone sales and generally the sales of tech products.

Another important topic of the agenda for 2022 and onwards has to be the one of 5G. First of all, the EU seems to be decided to push towards heavy investment in building the needed infrastructure, to fill the gap that exists with other countries. Not only that, but the European Union also needs to help national telecoms companies that are experiencing huge costs: to do so, the best course is to help them convince investors that 5G is a good opportunity for returns, especially in the current global landscape where the rush towards better and faster networks to provide more and more services seems inevitable.

We have already discussed how China and the United States are at the forefront of development in this field. The critical part is to decide who to entrust for the new critical infrastructures needed for 5G to work. The recent case of Germany clearly represents the current EU situation: it has taken two years, from 2019 to 2021 to rule who to entrust for this technology, particularly because of the implications of Huawei with the telecom infrastructures in Germany. Because of the legal issues Huawei had in the US, scepticism towards the safety of such partner spread in the national debate. It is clear that Germany, and broadly speaking the whole EU market, was not prepared to access the trustworthiness of its partners and suppliers. This is also one of the reasons behind the late development of 5G in the EU.

This raises another important topic, this time regarding the infrastructure of the Internet in the EU. Why doesn't the EU entrust European companies to do the job, effectively ensuring better safety, control, and accountability over such a critical issue? It appears that in the EU, if a national company does not play a role in the discussion, then any other option works, being it European but also from the US or China: national

politics does not seem to care about European companies, contributing to undermine the global relevance of these organizations, that may lag behind in size and thus have higher prices, but probably would create a better ecosystem in the long term. Ericsson and Nokia, respectively a Swedish and a Finnish company, struggle to get noticed because they respond to weak governments and to the EU regulation. Huawei, on the other hand, being based in China, has a strong hand laid towards it from Beijing's government, and has to deal with a much less strict regulatory framework.

Of course, all this has to be put in perspective: lobbying is again a very strong component and Huawei and Cisco have much more power to influence the opinion of politicians and the public and companies such as Deutsche Telekom, Telefonica and Vodafone advocated for their historic partner in Huawei. Proof can be found in a letter sent from Telefonica to members of the German parliament, that when compared with the actual data, appears to be extremely biased towards the Chinese company, making absurd claims on the quality and price to performance of Huawei services, not even taking into consideration other European companies[93].

Another issue that emerged is the influence that China's retribution power has on the EU market. Resisting to Huawei means to resist China, creating unfavourable market situations that could hinder future collaborations and hurt the already existing ones. This was made clear from China's ambassador to Germany in 2019:

> "Nice car industry you have there. Too bad if something happened to its sales in China"

Such a quote should help the EU taking more drastic decisions on the future of economic relationships with China and related companies. A strong position by the institutions could send a signal to all those companies that strongly rely on unreliable partners only because of costs, and taking into consideration the ethical, political and economic implications that could occur in case of international policy disputes, wars or new regulation.

[93] https://twitter.com/noahbarkin/status/1204819719259394054?s=20

The German case regarding 5G puts into perspective how much the Internet issue is becoming an interconnected in the global context. It is not just an issue of a technology, it is becoming a democracy issue, an economic issue, but also an ethical issue. There is also a component related to climate change: the ICT industry has still a huge carbon footprint in many sectors, and even if many tech giants advocate for net zero strategies and goals, there is a lot still to be done. The 2019 report of the ITU regarding climate change in the ICT sector[94], underlines the fact that circular economy could be a good strategy for high tech companies to help.

At the same time, the spread of new technologies such as 5G, IoT, Artificial Intelligence, Robotics and Cryptocurrencies etc. contributes to increase the number of data centres that rely on high power servers, that require a lot of energy to run. The mobile data flow is reaching greater and greater levels, with numbers reaching 11.5 Exabytes per month in 2017, almost doubling the 6.7 Exabytes per month observed in 2016: this is extremely expensive in terms of energy use[95].

The example of cryptocurrency, that led many people to build farms of graphics cards to mine Bitcoin and Ethereum, makes it clear that even among the common people energy consumption rises when new technologies and opportunities come along[96].

Moreover, the sheer number of products that enter the market everyday creates great amounts of waste that are hard to recycle; this along with all the waste of infrastructures that become obsolete, makes it for a great problem for the future: this is why ITU suggests circular economy practices to reduce the number of products that get thrown away without a second life. The figure below underlines the amount of e-waste, 44,7 million tonnes, that the sector generates in a year, putting it into perspective with two fitting examples.

[94] https://www.itu.int/pub/T-TUT-ICT-2019
[95] Cisco. (2019). Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2017-2022. Cisco.
[96] https://news.climate.columbia.edu/2022/05/04/cryptocurrency-energy/

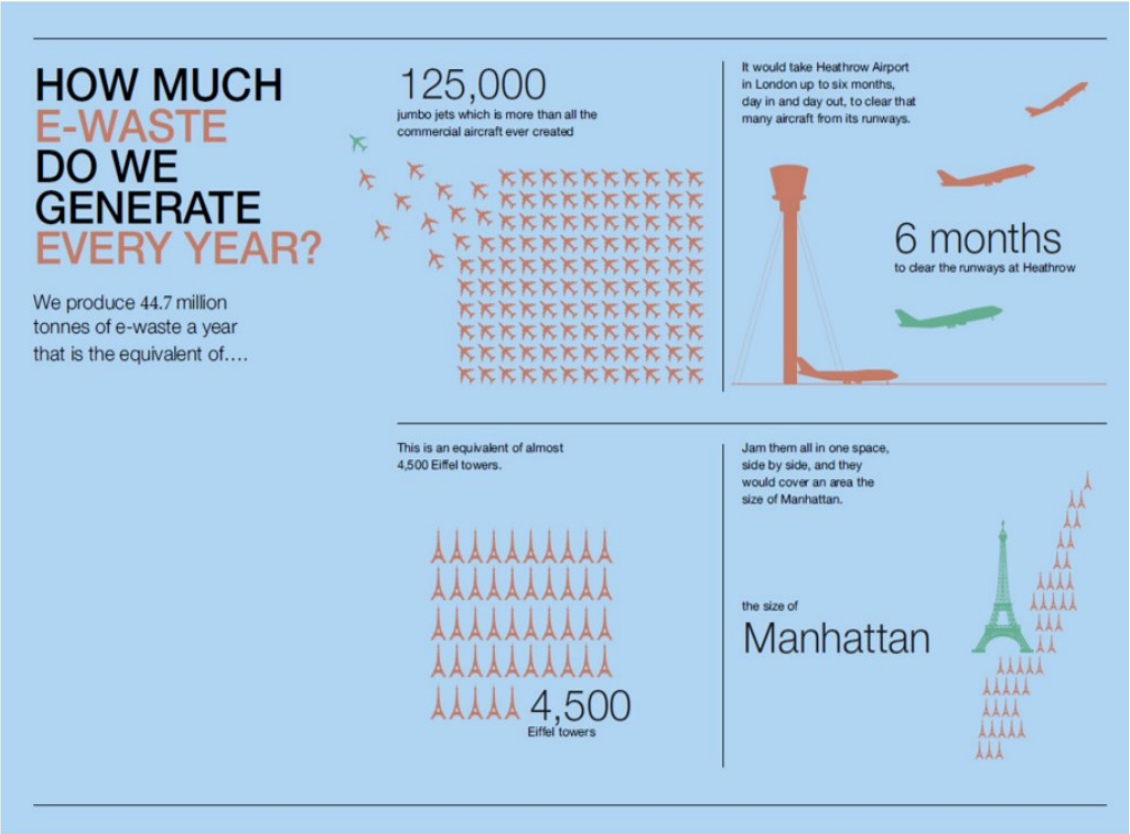

Figure 17. How much waste is generated each year? Sourced by the 2019 ICU report "Turning digital technology innovation into climate action"

But if there's a sector that can evolve and reduce emissions is ICT: research shows that the initial development and implementation of new infrastructures rises the energy costs and general CO2 emissions of the sector as a whole. This means that, in the current phase where the EU is still building new high-capacity networks and the infrastructures for 5G are being built, we are at the peak of a phase that will plateau once the technology is built and the whole sector settles[97]. In general, the effects should be positive after the initial phase, and there should be a reduction in overall emissions of 10 times the value of the emissions caused by the deployment phase. In order for this to happen though, climate change goals and generally sustainability needs to be a strong priority in this sector as well. Particularly, the ITU recommends that developing

[97] Hernnäs, H. (2018). What Is the Impact of ICT on CO2 Emissions? Ericsson. Sourced from: 8, www.ericsson.com/assets/local/about
-ericsson/sustainability-and-corporate-responsibility/documents/2018-09-helena-hernnas-m1-dissertation.pdf

countries start developing already mature technologies so that the general emission levels can be lower, enabling to reach the 2030 and 2050 goals.

This topic is quite debated though: there are researchers arguing that there will not be a plateau phase where the emissions will decrease. This is because if we take a look at the history of the sector, the process when implementing new technology has been the following:

1. At first ICT develops, becomes more efficient, so much that it becomes a significant player in the global economy. With such a great expansion, emissions rise massively, because of the need for deployment of the needed infrastructures.
2. Global emissions peaks, reaching high levels but briefly helps reducing emissions for a few years thanks to the technical innovations.
3. A new technology arises, and even if sustainability is taken into a consideration as a factor, economic interests are too strong to prevent emissions to rise again during the development of the new tech[98].

From both sides we can access that organizations must be targeted by regulators worldwide, including the EU, to enforce better sustainability in their practices, during all phases of the implementation of new technologies: particularly it should be assessed clearly how much a technology is going to positively impact emissions when launched, in order to give international organizations better tools to analyse who to entrust with funds, or generally have better data to analyse the sector.

It must be said that the EU in particular is committing to carbon neutrality under the Green Deal plan by 2050: a study from 2018[99] indicates that telecommunication networks will grow, in a timeframe of 9 years, by an alarming rate, creating issues that can only be solved with the right mix of objectives and regulation. Data centres are a

[98] Charlotte Freitag, M. B.-L. (2021). The real climate and transformative impact of ICT: A critique of estimates, trends, and regulations. CellPress.
[99] https://cordis.europa.eu/project/id/320013/reporting

fundamental target for the EU strategy, with carbon neutrality set for as early as 2030, using new and more efficient technologies, particularly relying on BESS systems working with renewable energy sources.

Finally, there's the issue of cryptocurrencies. Believe it or not, there is strong lobbying coming from the side of cryptocurrency related companies and organizations as well on related topics that could influence the market and its numbers have risen massively in the last two years, particularly in the US, where these practices are generally more common in comparison to the EU case. The sudden rise can be observed in Figure 18.

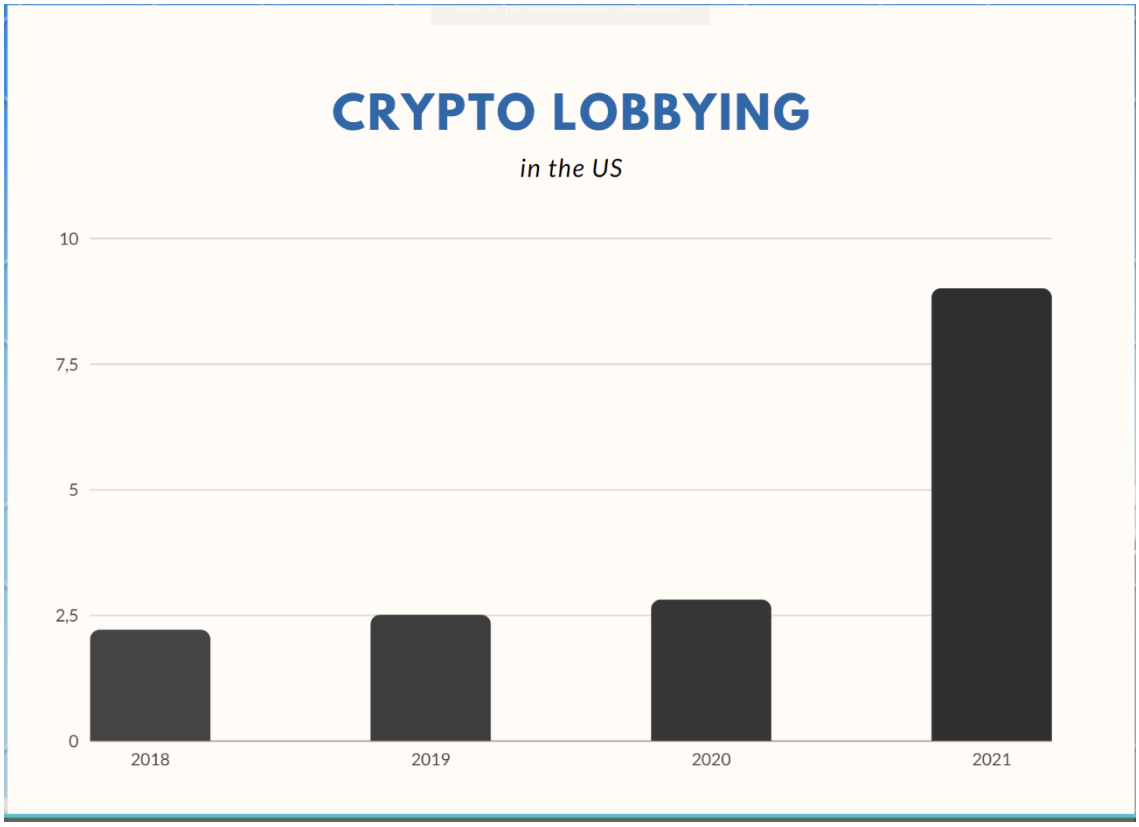

Figure 18. Lobbying expenditure through the years in the US in millions of dollars.

An instance of this occurred in April 2022, around negotiations around the Transfer of Funds Regulation which aims at regulating the crypto sector by tracking companies that use this type of currency to send or trade, creating a system that makes it mandatory to declare who will receive and who will send funds. This is to prevent money laundry

or shady practices exploiting the nature of such currency. Quickly, leaders of big Crypto related organizations such as Coinbase and Ripple attempted to get their reasons heard on the debate.

The general argument made by Crypto giants is that authorities are just pushing regulation without having the right knowledge about the present and future of such technology: this is shaping up very similarly to the case of service providers in telecommunication, where most of the knowledge comes from organizations that have interests in the market, in the form of reports and papers. These actors assess that a freeing alternative to traditional finance that enables regular people to reclaim control over their resources from large financial institution is the key to a better society. To make their case heard, these companies are organizing meetings, workshops, and webinars[100] that try to push the issues closer to the legislators but also common people[101].

Blockchain for Europe, an organization strongly in favour of Crypto that includes in the board representatives from Binance, Ripple, Blockseed, Ava Labs and Osom, recently called the TFR a "missed opportunity", discussing that:

> "The EU failed to advance future-proof regulation for our nascent blockchain industry which would have ensured consumer protection and position Europe as a global leader in the future Web 3.0 economy[102]".

The attempt is to, once again like the previous case we have discussed, to influence the trilogue negotiations before the summer break.

The "free crypto" message that these companies and organizations are sending is currently colliding with the scepticism about cryptocurrencies of the EU left parties, with great discussion – sometimes ending with Internet backlash towards the EU MEPs and representatives, like the case of Assita Kanko, who was publicly targeted from

[100] https://www.blockchain4europe.eu/
[101] https://www.politico.eu/article/crypto-campaign-target-eu-meps-transfer-funds-regulation/
[102] https://www.blockchain4europe.eu/news/ep-vote-on-transfer-of-funds-regulation-threatens-future-of-eu-blockchain-industry/

Internet trolls[103] - creating a rift inside the parliament. Many conservatives MEPs are, in fact, accusing their rivals with politicizing a technology that should be, according to them, fostered instead of suppressed. Inside the general discussion, two particular bills have heated up the discussion in these last few months: MiCA, that wants to establish safety and protection standards towards investors that are involved in the crypto market; Travel Rule, that tries to stop illegal financiers from laundering money with crypto – the aforementioned TFR -.

The issue of crypto is splitting so much the world of politics because it touches a key aspect of the society: the concept of economy. Bitcoin's attempt to establish a decentralized alternative to the current banking institutions and agencies seems to fit perfectly in the right's pro market idea of the society, and struggles to cope with the idea of a social economy, that is a prerogative in the left's way of conceiving society[104]. This also appears to be an issue that is seen more positively by the younger generations, that are more accustomed to the idea of Internet-based services – also of the financial kind – compared to the older generation: this explains why there are groups of left progressives that support crypto, particular the newer projects that have come up in the last few years.

There is also the concern regarding climate change and sustainability: to process blockchain transactions, cryptocurrencies use enormous amounts of power, in the form of farms and specialized computers that often are not specifically built for that purpose, and thus are quite inefficient. To put it into perspective, Bitcoin's blockchain is estimated to demand up to 15GW of power, that annually translates into 130TWh: more electricity than Sweden and Norway consume in a year[105]. Being climate change more of a left-wing concern, this adds up to the reasons for pushing back this kind of technology. The usual answer to these concerns is that the current banking sector consumes way more than the crypto counterpart, so there is nothing to worry about.

---

[103][103] https://www.politico.eu/article/crypto-lobbyists-condemn-industry-trolls-target-mep-oversight-rules/
[104] Golumbia, D. (2016). The Politics of Bitcoin. Minneapolis: University of Minnesota.
[105] https://www.energycouncil.com.au/analysis/cryptocurrency-drives-energy-demand/#:~:text=Bitcoin's%20global%20network%20of%20miners,just%20behind%20Egypt%20and%20Poland.

Regarding money laundering, we have already discussed about Travel Rule: analysing the political framework, the issue created divisions not only among different parties, but also inside the S&D and the Greens themselves. The key problem at stake is to understand if these types of controls are necessary for a market that is still small, or if energy and resources would be better spent to focus on the financial industry, that has way greater levels of illicit activities, when considering how big the market is. As we have already discussed, this issue received attention by lobbyists that are actively exploiting the revolving doors of Brussels institutions to gain knowledge and connections.

As far as the transparency register goes, the information that we can gather shows a collective spending of 650.000 EUR for lobbying in 2021 with just a few companies actively disclosing their activities.

Conclusions and final remarks

The Internet is one of the most complex, multi-layered tools that has never been conceptualized. Since it was first envisioned by the researchers working for ARPA in the form of a "Galactic Network", it has grown to become an interconnected system of computer networks, with each part having its own authoritative body, that takes decisions and establishes rules on the specific layer they are operating in. We now talk about digitalization and digital economy, with numbers that are increasing every year, and that skyrocketed during the pandemic because of the enforced need for a way to live and work remotely. The actors at stake have grown along with the growth of the Internet and each one of them plays a role in shaping the rules that guide us to the future of communication. And with more and more services available to end-users that integrate deep into their daily life, dealing with personal information and data, the EU felt the need for a strong regulatory framework to prevent illicit activities and to protect citizens.

Analysing the DSM and its specific regulation, we have identified a good chunk of the regulation that the EU has produced to tackle inequality, security, transparency, and market competitiveness: what we have observed is a good, even if at times incomplete, coverage of all the different issues at stake, with many decisions being considered inadequate by actors operating in the specific fields covered by these norms. The main issue appears to be a general lack of knowledge from the EU institutions, that struggles with such advanced and complex matters, creating a fertile ground for lobbying to fill the gaps, pulling decision making towards specific interests that not always are also the interest of the citizens. The fact that the market is fresh and up for grasp by investors globally, makes it a desirable target for organization that own the specific knowledge of these fields, and have the money to ensure that this knowledge stays in their hands. Big telecom companies used to shape decisions in the past, and now the role has been filled by Big Tech service providers, that have a great deal of power in decision making process and are able to exploit the weaknesses of the EU in terms of transparency through revolving doors and a badly implemented transparency register for lobbyists.

And there are so many new fields that are becoming more and more central: at the core of the political discussion we have new economic tools, such as cryptocurrencies, new infrastructures for the next generation of high-speed mobile connectivity in the form of 5G and AI. All EU decisions that are being taken and that will be taken in the following years regarding these topics are going to shape the future in a much stronger way than everything that came before it. It is important to ensure a democratic decision making, that takes into account all possible outcome and that operates for the good of the EU citizens. But as we saw, lobbying by private organizations is already very strong and has the potential to negatively impact the democratic nature of decision making, even more when the field is so complex and layered. The EU is walking the right steps, but the focus needs to be shifted on gathering the right knowledge on complex topics in advance, to avoid fighting on the backfoot against strong interests without the correct information to take decisions that work in favour of EU citizens.

BIBLIOGRAPHY

Abbott, A. B. (1999). The Liberalization of the Telecommunications Sector: A Rent-Seeking Perspective. *European Journal of Law and Economics*, 63–77 .

Andrews, D. C. (2019). The Best versus the Rest: Divergence across Firms during the Global Productivity Slowdown. *Mimeo*.

Ark, B. v. (2016). The Productivity Paradox of the New Digital Economy. *International Productivity Monitor*, 3-18.

Bates, S. J. (2018). In support of Internet entropy: mitigatin and increasingly dangerous lack of redundancy in DNS Resolution by Major Websites and Services. *NBER Working Paper 24317*.

Benkler, Y. (2000). From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access. *Federak Communication Law Journal 52*.

BEREC. (2020). *BEREC Work Programme 2021.*

Berners-Lee, T. (March 1989, May 1990). Information Management: A Proposal. *CERN*.

Blayne Haggart, N. T. (2021). *Power and Authority in Internet Governance: Return of the State?* London: Routledge.

Bloom, N. B.-E. (2019). What Drives Differences in Management Practices? *American Economic Review, Vol. 109, No 5,*, 1648-1680.

Bughin, J. (2011). *The impact of Internet technologies: Search.* Chicago: McKinsey & Company.

Campbell, D. F. (January 2017). The 5G economy: how 5g technology will contribute to the global eocnomy. *IHS ECONOMICS & IHS TECHNOLOGY*.

Charlotte Freitag, M. B.-L. (2021). The real climate and transformative impact of ICT: A critique of estimates, trends, and regulations. *CellPress*.

Cisco. (2019). *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2017-2022.* Cisco.

Clarke, A. C. (Feb. 1945). V2 for Ionosphere Research. *Wireless World*, 58.

Crompton, S. W. (2007). *Sputnik/Explorer I: The Race to Conquer Space.* Chelsea House.

Daniel Mikkelsen, H. S.-J. (n.d.). *GDPR compliance since May 2018: A continuing challenge.* McKinsey & Company.

EDRi. (2016). *Response to the European Ombudsman's public consultation on the transparency of trilogues.* Brussels: EDRi.

Er. Puneet, E. D. (July-Aug 2017). Cryptocurrency: Trends, Perspectives and Challenges. *International Journal of Trend in Research and Development, Volume 4*, 4-6.

European Commission. (2003). *The Role of eGovernment for Europe's Future [SEC(2003) 1038].* European Commission.

European Commission. (2015). *A Digital Single Market Strategy for Europe.* Brussels.

European Commission. (2016). *Commission paves the way for more and better internet connectivity for alla citizens and businesses.* Strasbourg: European Commission Press Release.

European Commission. (2021). *Digital Economy and Society Index* . Bruxelles: European Commission.

Farrand, B. (2015). Lobbying and Lawmaking in the European Union: The Development of Copyright Law and the Rejection of the Anti–Counterfeiting Trade Agreement. *Oxford Journal of Legal Studies*, pp. 487-514.

Feria, R. d. (2014). *LA RÉORIENTATION EUROPÉENNE DE LA TVA À LA SUITE DU RENONCEMENT AU RÉGIME DÉFINITIF.* Toulouse: Presses de l'Université Toulouse 1 Capitole, LGDJ - Lextenso Editions.

G. Kondova, J. E. (2020). Self-Sovereign Identity on Public Blockchains and the GDPR. *CM SAC Conference*, (pp. 342 - 345). Brno.

Garcia, L. K. (2021). John Rawls and the limits of net neutrality in the Internet market: new ethical insights for entrepreneurs. *Filosofía y Ciencias Sociales En Tiempos De Desconciert*, 1190-1205.

Golumbia, D. (2016). *The Politics of Bitcoin.* Minneapolis: University of Minnesota .

Hafner, L. (1998). *Where Wizards Stay Up Late: The Origins of the Internet.* New York: Simon & Schuster.

Harberger, A. C. (1998). A Vision of the growth process. *American Economic Review, Vol. 88, No. 1*, 1-30.

Hernnäs, H. (2018). *What Is the Impact of ICT on CO2 Emissions?* Ericsson.

Hillis. (1998). On the margins: The invisibility of communications in geography. *Progress in Human Geography*, 543-566.

Jacobides, M. G. (2020). *Regulating Big Tech in Europe: Why, so What, and How Understanding Their Business Models and Ecosystems Can Make a Difference.* London: London Business School.

Joseph P. Bailey, L. W. (1995). *Internet Economics.* Hattiesburg: MIT.

Kergueno, R. (2021). *Deep pockets, open doors. Big tech lobbying in Brussels.* Brussels: Transparency International EU.

Kleinrock, L. (1964). *Communication Nets: Stochastic Message Flow and Delay.* New York: Mcgraw-Hill.

Klimek, L. (2020). Misuse of Contactless Payment Cards with Radio-Frequency Identification. *Masaryk University Journal of Law and Technology*, 260-272.

Lehmann, W. (2003). *Lobbying in the European Union: current rules and practices.* Luxembourg: European Parliament.

Leiner, B. M. (2009). A brief history of the Internet. *ACM SIGCOMM Computer Communication Review, Volume 39, Issue 5*, 22-31.

Licklider, J. (1960). Man-Computer Symbiosis. *IRE Transactions on Human Factors in Electronics, Volume HFE-1*, 4-11.

Markowsky. (2018). *Token Frenzy.* London: GP. Bullhound.

Matthieu Pélissié du Rausas, J. M. (2011). Internet matters: The Net's sweeping impact on growth, jobs, and prosperity. *McKinsey Global Institute*.

McCraw, C. (2018). *American Business Since 1920: How It Worked.* Hoboken: Blackwell Pub.

McQuaid, K. (2007). Sputnik Reconsidered: Image and Reality in the Early Space Age. *Canadian Review of American Studies*, 371-401.

Metcalfe, R. M. (December 1973). *Packet communication.* Cambridge: MIT.

Milošević, N. e. (2018). Digital economy in Europe: Evaluation of countries' performances. *Zb. rad. Ekon. fak. Rij.*, 861-880.

Morrison and Foerster. (2018). *EU Digital Market VAT Reform.* San Francisco.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Pathak, S. (2013). *Evolution in generations of cellular mobile communication.* Bhopal: National Law Institute University, Bhopal.

Raja, A. L. (2021). Ultrafast optical circuit switching for data centres using integrated soliton microcombs. *Nature*.

Robert Anderton, V. J. (2020). The digital economy and the euro area. *ECB Economic Bulletin*.

Roberts, L. G. (Nov. 1978). The evolution of packet switching. *Proceedings of the IEEE,*, 1307-1313.

S. Greenstein, M. P. (2016). Net neutrality: a fast lane to understanding the trade-offs. *American Economic Association*, pp. 127-150.

Savić, D. &. (2018). Challenges of General Data Protection Regulation (GDPR). *Sinteza 2018* (pp. 23-30). Beograd: Singidunum University.

Schein, V. E. (1977). Impact of flexible working hours on productivity. *Journal of applied pshychology*, 460-467.

Sebastian Engels, J. B. (2017). *The Portability Regulation (Regulation (EU) 2017/1128): A Commentary on the Scope and Application.* Journal of Intellectual Property, Information Technology and E-Commerce Law.

Solum, L. B. (2003). The Layers Principle: Internet Architecture and the Law. *Social Science Research Network Electronic Paper Collection*.

Squire Patton Boggs. (2019). *The EU Electronic Communications Code.* London: Squire Patton Boggs.

T.W. Hazlett, J. W. (2017). The Effect of Regulation on Broadband Markets: Evaluating the Empirical Evidence in the FCC's 2015 "Open Internet" Order. *Springer - Review of Industrial Organization*, 487–507.

Tian, H. J. (2021). The Economic Impact of Internet Connectivity. *INSEAD*.

Tomsho, G. (2016). *Guide to networking essentials.* Boston: Course Technology.

Wahl, T. (2019). *New Directive Criminalises Fraud and Counterfeiting of Non-Cash Means of Payment.* eucrim.

SITOGRAPHY

https://www.telegraph.co.uk/technology/news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.html

https://web.archive.org/web/20120609074456/http://ec.europa.eu/dgs/information_society/connect_en.htm

http://ec.europa.eu/dgs/information_society/connect_en.htm

https://cor.europa.eu/en/about/Pages/default.aspx

https://www.eesc.europa.eu/en/about

https://ec.europa.eu/info/priorities/state-union-speeches/state-union-2015_en

https://oeil.secure.europarl.europa.eu/oeil/search/search.do?searchTab=y

https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32017L2455

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0713

https://eur-lex.europa.eu/eli/reg/2016/679/oj

https://gdpr.eu/what-is-gdpr/?cn-reloaded=1

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R2286

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:171:0032:0040:EN:PDF

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:172:0010:0035:EN:PDF

https://eur-lex.europa.eu/eli/reg/2017/1128/oj

https://eur-lex.europa.eu/eli/reg/2017/1953/oj

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018R0302

https://www.eurocommerce.eu/media/155816/eurocommerce_faq_on_the_implementation_of_the_geoblocking_regulation_readonly.pdf

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32018R0644

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1724

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807

https://eur-lex.europa.eu/eli/reg/2019/881/oj

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R1150

https://www.osborneclarke.com/insights/regulation-eu-20191150-new-rules-protect-business-users-online-intermediation-platforms

https://digital-strategy.ec.europa.eu/en/library/declaration-future-internet

https://sdgpulse.unctad.org/ict-development/

https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

https://handlingar.se/en/request/digital_services_act_digital_mar_2#incoming-2249

https://corporateeurope.org/en/2022/04/big-techs-last-minute-attempt-tame-eu-tech-rules

https://corporateeurope.org/sites/default/files/2022-04/I2021_01055-66%20Overall%20Trialogue%20priorities%207854189_1_1_Google%2028%20feb.PDF

https://corporateeurope.org/sites/default/files/2022-04/Minnesanteckningar%20Google%2022%20feb%202022%20en-GB.pdf

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN

https://etno2021.live.ft.com/agenda/session/590008

https://www.euractiv.com/section/data-protection/news/european-parliament-calls-for-infringement-procedure-against-ireland/

https://www.europarl.europa.eu/news/en/agenda/briefing/2021-03-08/16/meps-expected-to-seek-an-end-to-remaining-geo-blocking-restrictions

https://www.pagero.com/news/european-parliament-vat-requirements/

https://twitter.com/noahbarkin/status/1204819719259394054?s=20

https://www.itu.int/pub/T-TUT-ICT-2019

https://news.climate.columbia.edu/2022/05/04/cryptocurrency-energy/

https://cordis.europa.eu/project/id/320013/reporting

https://www.blockchain4europe.eu/

https://www.politico.eu/article/crypto-campaign-target-eu-meps-transfer-funds-regulation/

https://www.blockchain4europe.eu/news/ep-vote-on-transfer-of-funds-regulation-threatens-future-of-eu-blockchain-industry/

https://www.politico.eu/article/crypto-lobbyists-condemn-industry-trolls-target-mep-oversight-rules/

https://www.energycouncil.com.au/analysis/cryptocurrency-drives-energy-demand/#:~:text=Bitcoin's%20global%20network%20of%20miners,just%20behind%20Egypt%20and%20Poland