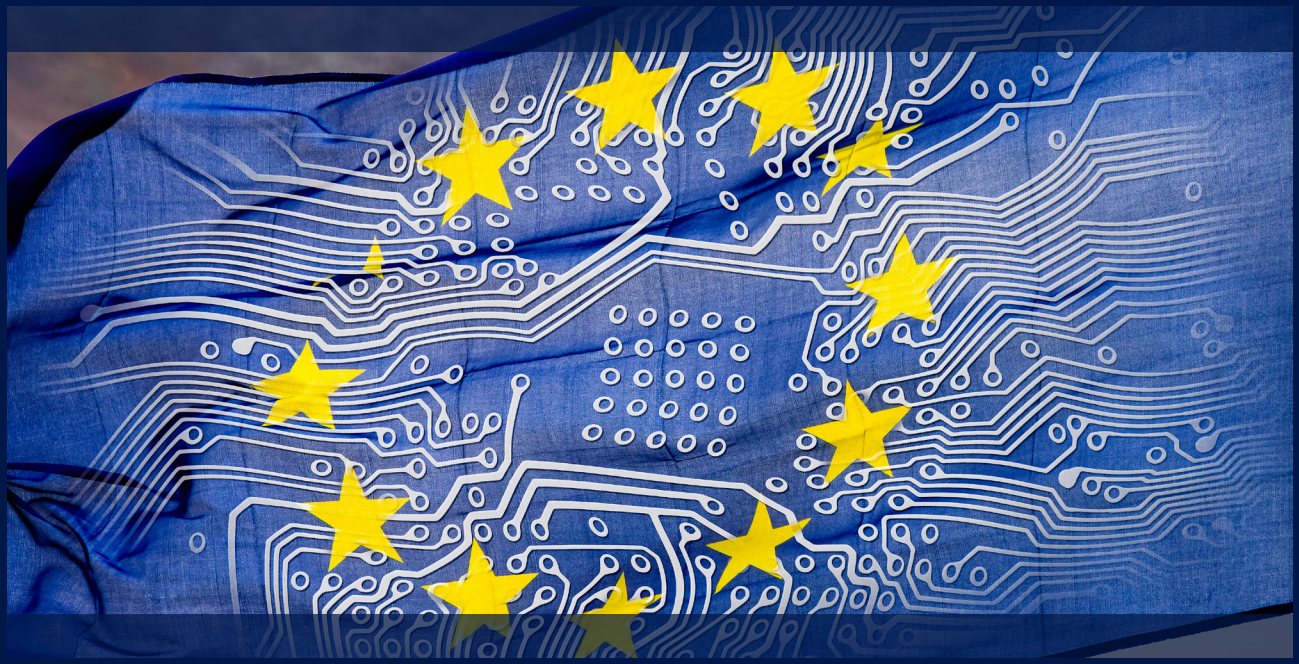
EUROPEAN DIGITAL INFRASTRUCTURE AND DATA SOVEREIGNTY

A POLICY PERSPECTIVE



CONTENT

EXECUTIVE SUMMARY

Recent discussions around 5G and COVID-19 contact tracing amplify the need for European sovereignty when it comes to digital infrastructures and the handling of data. This report provides an overview of policy motivations, trends, instruments and the role of various actors that jointly create the digital reality.

With the aim to develop policies that will contribute to a stronger European sovereignty when it comes to digital infrastructures and handling of data, a scenario-based framework representing policy choices is introduced that allows the assessment of these scenarios with respect to policy objectives. It is important to recognise that digital infrastructure control and data regulation are complementary and can be combined in various ways. Thus, the framework contains four different scenarios derived from combining opposite approaches with respect to infrastructure control and data regulation. The scenarios are then assessed with respect to their impact on the policy objectives growth, fairness, innovation potential, citizens trust, and level playing field.

The impact assessment serves as a high-level guidance for concrete policy development, and as such it provides an important tool for the development of digital infrastructure and data policy instruments. Europe is called upon, through coordinated action between the EC and the Member States, to virtuously connect *makers* (industry) and *shapers* (authorities, citizens) in order to create the right policy instruments for a sovereign European digital reality with innovation enhancing regulation that respects European values and rights while creating equal economic opportunity for all actors.

CONSIDERATIONS WITH RESPECT TO DIGITAL SOVEREIGNTY

The topic of European digital sovereignty has gradually emerged as a result of the increasing dominance of non-European actors in the so-called platform economy. Europe increasingly realises the importance of policies with respect to digital infrastructure and data handling to realise European digital sovereignty. The recent debate around 5G infrastructure deployment for example focussed on the geopolitical dimension of supplier choice.

This report appears during the unprecedented COVID-19 pandemic, which acts both as a magnifying glass and an accelerator. As a magnifying glass, since it shows in a magnified way the need for digital sovereignty in order to own and protect digital infrastructures and address privacy concerns in society. This lack of European digital sovereignty is, for example, clearly illustrated by the European struggle with COVID-19 contact tracing apps where European countries have to adapt their contact tracing approaches to solutions provided by US tech companies. As an accelerator since in many parts of the society a steep increase of digital infrastructure use is taking place due to the shift of activities on-line as a result of the world-wide lockdown. This shows how vital digital infrastructures and data have become for our society and economy.

ECONOMIC CONSIDERATIONS

Digital infrastructures and data are at the heart of digital platforms driving the digital transformation in both consumer environments (such as for example Social Media), and industrial environments (such as for example the Fourth Industrial Revolution). The data-driven digital transformation is a main source of innovation and produces wide benefits for consumers that escape GDP measurement (Brynjolfsson et al., 2019), since many digital goods have zero price and as a result the welfare gains from these goods are not reflected in GDP or productivity statistics.

World-class connectivity in 5G will be a key enabler of Europe's digital economy. It can boost digitization of services and industrial processes, cutting costs and increasing efficiencies (See Palovirta & Grassia, 2019). According to a market research report (Campbell et al., 2017), 5G will generate USD 12.3 trillion of global economic output by 2035 and that Investment in the value chain is expected to generate a further USD 3.5 trillion in output and provide support for 22 million jobs. The Internet of Things (IoT) will have a huge impact on industrial and service processes, climate control, urban environments, health care and many other facets of life. The network infrastructures form the basis for cloud infrastructures that create global integrated platforms supporting ubiquitous services and data access.

Modern Artificial Intelligence (AI) extracts value from data. More and better data means more accurate AI models, which in turn means potentially more benefits to society and business. AI will lead to a transition in production processes, producing significant economic growth and increasing economic output. This is summarised in a recent brief of the European Parliament on the economic impact of AI (European Parliament, 2019b). In this brief Accenture predicts a major productivity breakthrough of doubling annual global economic growth by 2035, PwC predicts a 14% growth of global GDP by 2030 and McKinsey Global Institute estimates an

additional economic output of around US$13 trillion by 2030, increasing global GDP by about 1.2 % annually.

Cybersecurity plays an important role when it comes to realising the economic benefits from digitalisation, as Von der Leyen, European Commission president, noted: *"Cybersecurity and digitalisation are two sides of the same coin. This is why cybersecurity is a top priority. For the competitiveness of European companies, we have to have stringent security requirements and a unified European approach."*

A study estimated that the economic impact of cybercrime in the Union amounted to 0.41% of EU GDP (i.e. around EUR 55 billion) in 2013 (CSIS, 2014); with Germany being the most affected Member States (1.6 % of GDP). As a result of these concerns, the global cybersecurity market is predicted to grow at a compound annual rate of 10% and be worth over $200 billion by 2021 (Morgan, 2015).

SOCIETAL CONSIDERATIONS

Cyber threats and attacks have also become closely linked to the privacy and data protection issues (European Commission, SWD(2017) 500). At the same time the data economy is generating several major societal concerns. Cybersecurity is a strong concern in relation to both infrastructure and data. Privacy concerns are raising in everyday life. The EU Ethics Advisory Group has in 2018 expressed concern on the relationship between personhood and personal data, the risks of discrimination as a result of data processing, and the risks of undermining the foundations of democracy. In Europe, GDPR is a regulatory intervention to address some of these concerns. We see also support for the principles of GDPR in the US, with Microsoft being one of the proponents of a US GDPR, and the introduction of the California Consumer Privacy Act (CCPA), effective from 1 January, 2020.

Concerns are also expressed on equitable access and persisting digital exclusion and divide. The digital transformation and revolution is not yet reaching everyone and the digital divide is taking new forms. Digital innovations still do not reach everyone, as digital divides still exist, especially as those "who lack safe and affordable access to digital technologies are overwhelmingly from groups who are already marginalised: women, elderly people and those with disabilities; indigenous groups; and those who live in poor, remote or rural areas" (United Nations, 2019, p. 11-24). Developments in digital technologies do not therefore take place in a vacuum, and the values that guide technological development must be set out clearly. The "application of technology must be aligned with investments in human capital, infrastructure and environmental protection" (United Nations, 2019, p. 15). With specific regard to 5G, while a viable case for deployments of these new networks can be made for densely populated urban areas, there is a risk that rural and suburban areas get left out (Ibid).

GEOPOLITICAL CONSIDERATIONS

Next to the societal concerns there are international incidents and increasing geopolitical tensions. The German Ministry of Economy (BMWi, 2019) presented the project Gaia-X – a European cloud aiming to provide *"the next generation of data infrastructure for Europe: a secure, federated system that meets the highest standards of digital sovereignty while promoting innovation"*. Technological sovereignty also figures high on the agenda of the new European Commission. In general, one observes that one of the drivers of cybersecurity policy is to be a stronger global actor in trade, development cooperation, defence and international diplomacy (Timmers, 2018).

Also, when it comes to data, China and the United States are each large, single markets, enabling the gathering of giant quantities of data to fuel their algorithms, whereas Europe is more fragmented (O'Hara and Hall, 2018). As a consequence, the US and China are leading the data 'refinery': the AI research and applications and specialised chips that run them, to produce results (profiles,

predictions, etc). In the last 15 years the battle of domination in the digital landscape has led to the oligarchy of the American GAFAM, their Chinese counterparts (Alibaba, Baidu, Tencent, et al.) and other emerging, typically non-European, platforms. ETNO, a major European telecoms association, urges the European digital agenda to focus on IoT, 5G, and AI to close the gap with the US and China.

The European model is value- and human rights-based and focuses on ethics and privacy. The GDPR has enshrined into EU law a universalistic approach to the protection of privacy, extending protection of its citizens in other jurisdictions and enlarging the right to be forgotten. GDPR covers all data processing activities to anticipate and minimise risk. Also, in recent years the EU competition approach has been more proactive including anti-trust initiatives against dominant firms, based on Article 102 of the EU Treaty.

The US model leans in the American tradition more toward liberty and is a mix of a technology and commerce driven approach. With respect to privacy the dominant view is to treat it as tort, where the victim must prove the harm, which is in line with the Silicon Valley attitude to disrupt and move fast before regulation intervenes (Zuboff, 2019). In this respect the approach is commercial and there is convergence of views between Silicon Valley and Washington. One characteristic of the US model is the lack of a unified federal framework for data protection and cyber security and the presence of several state laws and other sources of regulation or self-regulation and standardisation. It is remarkable though that, as a result of Europe introducing GDPR and other measures, there is mounting pressure in the US for a federal standardisation on data privacy and cybersecurity.

The Chinese model promotes its own tech giants (Baidu, Tencent and Alibaba) which work under close governmental control. These companies are less complacent, more vigorous, more eager for competition, and less constrained than their US or European counterparts. An important advantage of China is also its implementation capacity. China has the advantage in terms of both the national skillset and the numbers of scientists it can deploy (Lee, 2018). Data protection in China is not up to European standards in terms of values and rights. China's cybersecurity market is, to all intents and purposes, driven by government prerogatives. It is dominated by large monopolies with strong links to national security with probably negative effects on the provision of cybersecurity (Cheung, 2018). Moreover, its Internet economy generates far more data than any other. Lastly, unhindered by data protection regulation or noticeable public demand for privacy, data is gathered from many other sources, including closed circuit television.

Hence, one could conclude that Europe can win strategic autonomy by focussing policy on human rights, building trust in society through good data protection and cybersecurity, and initiating trust policy to improve competitiveness. Public acceptability and trust, both nationally and internationally, are key for the deployment and adoption of new emerging technological possibilities from which tangible benefit may accrue. Generalised and systemic trust, with the underpinning social capital, are the social glue that enables collaborative and productive practices in the digital ecosystem, in particular in the European model.

DIGITAL INFRASTRUCTURE CONTROL TRENDS AND DEVELOPMENTS

5G networks, although still not mature and consolidated, are deemed crucial to secure the strategic autonomy of the Union (NIS Cooperation Group, 2019). Europe has taken various policy actions, including the EC Recommendation on Cybersecurity of 5G network (EU 2019/534), the 5G Action Plan (COM(2016)588), setting 2020 as the target for roll-out of commercial 5G networks through a mix of private and public investments. But a more balanced view is needed, including cybersecurity and the EU's strategic position in the global competitive and geopolitical landscape (Albrycht & Swiatkowska, 2019). Critical infrastructures on 5G could be disrupted by intentional hostile breaches or may end up being too dependent on suppliers from third countries.

In the case of the Internet of Things (IoT), the critical security and data protection issues are similar to 5G. While capital investment is less of an obstacle, lack of standards and of business models certainly is. With full deployment of 5G and IoT, real-time processing will be possible with 5G and Edge Cloud computing. Decentralised processing may also be needed for compliance with intellectual property and/or data protection. 5G and IoT in combination with cloud computing will increase the surface of attack and vulnerabilities related to massive data processing and increasing device connectivity. IoT will have a huge impact on automotive, industry, retail and smart building equipment. The large trove of data generated by IoT connections and devices will create fresh resources for growing data analytics and AI in Europe (Palovirta & Grassia, 2019). IoT will also further accelerate networking of individual industries and infrastructure sectors. Competing industry coalitions and platforms are emerging with many different infrastructures that need to form IoT networks (Walport, 2014), which adds to the challenges of adequately protecting data.

Cloud computing encompasses infrastructure (e.g. processing, storage, communication), platforms and software. Interoperability is one of the key advantages of cloud computing allowing implementation of services and streamlining data gathering and processing. From a sovereignty perspective the main challenge is the tension between the technological independence of the location of storage on the one hand, and national regulations on storage locations and data ownership and data protection on the other hand. In Europe, non-EU cloud infrastructure providers currently account for about 80 percent of the global market (Palovirta & Grassia, 2019). Cloud computing also presents challenges when fully integrated seamlessly with 5G and IoT (and considering use of AI algorithms).

The growth of platforms has led to worries of data abuse, privacy violation and proper distribution of profit generated by data (Lee et al., 2017). Data governance within platforms, where there are multiple parties contributing, deriving and using data, complicates ownership, access, usage and profit-sharing of collected and derived data. These complexities lead to a larger attack surface and decrease of trust. The US and China dominate the data-rich intermediation layer. The Top 25 platforms (mostly from US or China) attract most of the visits and, most likely, most of the data. US platforms receive traffic and data from most countries. Overall, most traffic goes to US sites, about a third to national sites, and a tiny portion to sites of third.

DATA PROTECTION TRENDS AND **DEVELOPMENTS**

Digital infrastructures play an important role in the collection and processing of data and the products derived from the data. Much of this data is personal and called by Zuboff (2019) 'behavioural surplus' that users don't even realise are collected about them. The loss of control over personal information creates risks for individuals that are difficult to understand and value (Cohen, 2019). Behavioural data may not be legally defined as personal, but the GDPR tends to expand the definition. How industry is harnessing big data to transform personal digital data into economic value, has been described by Cohen (2012, 2015) as the latest form of 'bioprospecting'. Concerns over feedback loops based on surveillance of online users have also emerged (Zuboff, 2019). Users struggle to manage their privacy relations with all digital service providers they interact with online, cannot assess the risk of harm in a series of isolated transactions given that many privacy harms are cumulative in nature (Solove, 2013).

The introduction of the GDPR has being very influential and highly debated in the field of data protection. Advocates of decentralised models and subject sovereignty call for more; others criticise it as either unfeasible or as potentially stifling innovation. From both legal and technical perspectives, the right to withdraw consent, the right to be forgotten, and the right to explanation remain controversial both in terms of their feasibility and their potential disruption of existing practices and business models (Buiten, 2019; Goodman & Flaxman, 2017; Li et al., 2019; Politou et al., 2018; Wachter et al., 2018). Nevertheless, there is globally an increasing growth in data protection laws, many of which have been modelled on comprehensive guidelines or regulation such as the EU GDPR, or the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. According to UNCTAD, over 100 countries around the world now have data protection laws in place.

The main objective of data governance is to put in place authorisation policies for *roles and processes* to ensure that the data assets of an organisation can be effectively used by the organisation to fulfil its mission. Data governance policies can dictate who has access to what data, how such data can be used by which party, whether data can cross systems or borders, how data quality is established, what processes are in place to ensure data integrity, what happens when there is a data access breach or when data quality is compromised. Another fundamental aspect of data governance is identity management for individuals, organisations and resources involved. Identity is key for access control policies, for identifying data assets and where they are stored, and for establishing trust between parties. Cloud platforms, like Amazon Web Services and Microsoft Azure, provide support for Identity Access Management functionality to their customer enterprises.

AI has raised serious questions about accountability, fairness, bias, autonomy and due process of AI systems. The roots of biases in machine and deep learning are in data, testing, and decision models used. It is not only quantity, but also quality of data that defines validity and accuracy of the results (Domingos, 2012). If key data is withheld by design or chance, the algorithm's performance might become very poor (Olhede & Wolfe, 2017). The online marketing practices based on big data analytics reduce the autonomous decisions of consumers (Yeung, 2017). A key challenge for AI algorithms is how to address their potential biases and discriminatory effects. This holds particularly for AI surveillance tools and AI for cybersecurity. These issues are important for all infrastructures developments as well as related data protection and has clear implications for Europe's strategic digital autonomy.

THE ACTORS IN THE DIGITAL WORLD

A general policy position taken by free-market supporters in the innovators-regulators debate is that any attempt to regulate the current digital transformation would stifle innovation and produce undesirable side effects. In this position, for the sake of economic growth and innovation, matters should be deregulated and/or their governance should be devolved to the private sector through various forms of self-regulation and de *facto* standardisation. However, historically, it has been amply demonstrated that markets are never able to create by themselves the legal and institutional basis needed for their functioning and that the *Great Transformation* from rural to industrial society was to a large extent made possible by the institutional innovation produced by the state (Polanyi, 1957). In all situations where *"private industry could not or would not act, the public sector would provide the physical roads, ramps, and rails over which the traffic of commerce could move"* (Deloitte, 2017). This applies to some of the pillars on which the current digital transformation rests and which are taken for granted (Mazzucato, 2015). Many of the components included inside smart phones and the GPS technology exist thanks to very large public sector investments. Therefore, the digital transformation is driven by the interaction of *makers* (industry) and *shapers* (authorities, citizens).

Makers include technology and solution providers: technology developers, communication service providers, digital service and content providers, as well as hardware and software manufacturers (infrastructure devices and equipment, system software and support component manufacturing). Makers often organise themselves in industry associations and industry dominated standardisation bodies. They sometimes move before regulation and create infrastructural solutions and de-facto standards that may be hard to undo.

Key makers include the dominant platforms and tech giants both in terms of infrastructure and data, but also fast-growing start-ups and scale-ups, the so-called unicorns. With respect to communication infrastructure Europe still has two dominant players, Nokia and Ericsson, although their position is challenged by US and mainly Chinese competitors, such as Huawei. Mobile handsets, however, are fully dominated by US and Asian handset manufacturers combined with almost full US mobile operating system dominance. The global landscape of telecom operators is still quite divers, with especially in Europe a very fragmented landscape with many national players and few giants like Deutsche Telecom, Telefonica, Vodafone and Orange. In data platforms the US dominates through GAFAM, although these five enterprises are not a unified block, since there is a clear difference both in business model and in level of access to data (and advancement on machine learning).

Cyber security suppliers are diverse (Aggarwal & Reddie, 2018): cybersecurity firms, internet technology firms, and internet-adjacent firms. Cybersecurity firms provide products and/or services (i.e., Darktrace, FireEye, Palantir, Qadium, Kaspersky Lab, Symantec, F-Secure, etc.). Internet technology firms are heavily involved in the 'big data' space, and may use solutions from cybersecurity firms or produce their own. 'Internet-adjacent' firms have digital components but have the core business outside the technology sector, like Philips, Siemens, Thales, but also software companies like SAP and ATOS, working in domains such as medical, industrial, defence, or public services that have high security

and privacy requirements. Finally, a particular class of firms that will rely increasingly on IoT, are companies that manage critical infrastructures, such as for example energy companies: these may have special cybersecurity needs and may in the future produce their own solutions.

Shapers play a major role with respect to digital infrastructure, mainly in defining the specifications and regulating them. These include governments as well as other public sector actors, and citizens. Governments usually have a principal role in policy making and regulating. Other non-governmental agencies may also play a role, such as multiple stakeholder associations, NGOs, international and standardisation organisations. Citizens play a role through their voting and purchasing powers.

Governments seek to balance the interests of the users/citizens and of economy and society as a whole. This relates to e.g. equal access to innovation opportunities, data protection and security, consumer protection and competition. Government objectives can be seriously challenged by tech giants' interests and lobbying strategy (Codagnone, 2017; Codagnone et al., 2018) to defend commercial interests, for example in the debate around the open Internet and the interest of users receiving free services (Zuboff, 2019).

As shapers in the digital economy, authorities have been quite active when it comes to infrastructure regulation understanding that this can have a multiplier effect on economic output both in the short and long term, and digital infrastructures are considered key drivers of competitiveness. The technology area under consideration spans from mobile and fixed communication (spectrum, coverage, roll-out of 5G), Internet (net neutrality, domain name systems), data storage and management systems, cloud computing and data centres, applications, artificial intelligence (AI), Internet of Things (IoT), cybersecurity, and platforms.

Concerning data, the EU established as a first (and only) worldwide regulation for the protection of personal data (GDPR) which came into effect in May 2018. GDPR is joined by legislation for the use and reuse of public sector data (PSI: Public Sector Information), digital copyright, e-privacy and cyber security. Further steps on the regulatory framework for the use and re-use of privately-owned data are currently under discussion.

Although the public opinion focusses mainly on personal data, the future of the European Data Economy and of European Industry 4.0 also heavily depends on 'machine data' (including sensor data) which is expected to increase exponentially with full development of the IoT. The EU Regulation on the free flow of non-personal data (referred to as FFD Regulation) applicable as of 28 May, 2019 aims to remove barriers to the free flow of non-personal data to foster the data economy. Later the Commission issued a guidance to explain how the FDD regulation and GDPR interact and it discussed the concept of mixed datasets (comprising both personal and machine data), which will become increasingly common in AI and big data analytics. Currently, the interaction between the GDPR and FDD remains a thorny issue for mixed datasets. Non-personal, e.g. machine data, manufacturing data etc. and its role in technology innovation requires further analysis but is left outside the scope of this report.

Finally, a brief of the European Parliament on the EU ethical framework of AI, after describing its human-centric nature, adds: *"While this approach will unfold in the context of the global race on AI, EU policy-makers have adopted a frame of analysis to differentiate the EU strategy on AI from the US strategy (developed mostly through private-sector initiatives and self-regulation) and the Chinese strategy (essentially government-led and characterised by strong coordination of private and public investment into AI technologies). In its approach, the EU seeks to remain faithful to its cultural preferences and its higher standard of protection against the social risks posed by AI – in particular those affecting privacy, data protection and discrimination rules – unlike other more lax jurisdictions"* (European Parliament, 2019c).

COMBINING AND BALANCING INTERESTS IN THE DIGITAL WORLD

States in the European Union are democracies that implement a separation of powers when it comes to governance of the state. Typically, the separation is according to the 'trias politica' model, where legislation, execution, and jurisdiction are separated with independent powers and responsibilities. Regarding policy development and legislation thereof there is typically a collaboration between the execution power, government, and the legislation power, parliament to achieve specific objectives.

Policy objectives contain inherent dilemma's, such as innovation-regulation or value-economy. Tension between values and economic interest or state interest become visible from opposing claims and discourses emerging in the public debate, as well as the instrumentalization of digital infrastructures and law by either side. Neither 'leave it to the market' nor 'make it a public utility' are perfect in representing the full gamut of values, economic interests, and state priorities. Totally unregulated digital infrastructures and data protection do not automatically ensure distributed innovation nor equitable economic opportunity and growth. In the same way interventionist regulation on both digital infrastructures and data protection would not necessarily produce the desired outcome and may as well delay innovation if not well calibrated and implemented in a specific way.

In the development of policies regarding the digital world, we observe a mix of pro-active and reactive policy developments. Nevertheless, given the fast and often intangible developments in the digital world, policy development is also often reactive. This is important because it means that actors in the digital world such as businesses, service providers, and users play an important role by creating a de facto digital world. Dissatisfaction with such a de facto created digital world than often leads to policy development in order to create a more de jura digital world. When looking at the overall development of the digital world we see it is an interaction between makers and shapers, where makers create, and shapers regulate. The evolution of the digital reality is again a complex process, where the key actors are governments, business, citizens and regulators.

Makers and shapers should work hand in hand, since using a fully free-market approach to the current digital transformation in practice is not neutral. First, this would keep intact those uncertainties that delay innovators. Second, it would de *facto* reinforce and crystallise current trends and situations of market power that distort competition and impede new and more distributed forms of innovation (see report of the UK Digital Competition Expert Panel on 'Unlocking Digital Competition' and of the German Data Ethics Commission). Third, protectionism can be the result of both over-regulation and under-regulation. While some of the recent European regulatory initiatives and plans are introduced also with the transparent aim of increasing the competitiveness of European industries, it is also evident that US positions on data protection and anti-trust *'have permitted a race to the bottom in the accumulation of platform power and that the relative US laxity has disadvantaged European Internet businesses'* (Cohen, 2016; Cohen, 2019). One may therefore conclude that the current digital transformation requires a bottom up rethinking of competition and public utility regulatory regimes (Cohen, 2019). In many digi-

tal domains, also on net neutrality, we see on one hand industry players asking the freedom to experiment with new premium service business models for the sake of innovation. And on the other hand, consumer advocates and small Internet companies responding that price discrimination in the context of closed and dominant platforms threatens distributed and decentralised innovation and freedom of expression. The debate boils down to whether *"regulatory institutions should be designed to promote enhanced public accountability or whether instead they should take on configurations more responsive to informational capitalism's needs and goal"* (Cohen, 2016). In the US, Elizabeth Warren proposed: a) to unwind anti-competitive tech mergers such as Facebook's acquisition of WhatsApp; and, especially b) that online marketplaces which generate annual global revenues of more than USD25bn be declared 'platform utilities' and prohibited from both owning a platform and doing business on it. Related ideas are discussed in the European Commission in the context of competition rules. We also see the suggestion that Facebook, with its increasing influence on the political process, is de *facto* becoming a public utility (Susarla, 2018) .

If we look at the possible future integrated development of 5G, IoT, and Edge Cloud computing, a number of considerations can be made that may justify calls treating this combination as a new public utility digital infrastructure (Deloitte 2017). High investment needed for the deployment of 5G networks, leads to uncertainty on profitability and may discourage to deploy 5G or to do so only in profitable densely populated areas excluding rural areas. IoT deployment misses a foundational standardised infrastructure and the growth of connected IoT devices will create strong pressure on the allocation of existing spectrum needing government support. The convergence of 5G, IoT, and Edge Cloud computing will generate huge amounts of decentralised data, adding to already existing challenges and concerns about security and protection of personal data and privacy. The implications on strategic digital autonomy and external dependency determine Europe's choices on standards for 5G, IoT and cloud needed to avoid and minimise dependencies which could result in cybersecurity breaches by third countries, especially those that are not like-minded.

For 5G the current capital investment bottleneck is an opportunity for policymakers to support deployment and, consequently, lead and steer the process through regulatory requirements. Policy-makers *"can use a range of legal and regulatory actions to facilitate 5G network deployment. These include supporting the use of affordable wireless coverage (e.g. through sub-1 GHz bands) to reduce the digital divide, commercial incentives such as grants, or PPPs to stimulate investment in 5G networks"* (ITU, 2019). Governments, also being a user, can provide good use cases on these infrastructures establishing good practices to build trust and confidence in emerging digital technology.

A key policy question is whether data flow imbalances make a difference in national economic trajectories. It has been argued that directionality and content is irrelevant because data flows circulate ideas, research, technologies, talent, and best practices around the world. Moreover, the claim that 'open is best' has been used by US tech giants against EU regulation and the digital service tax. Another position is what Weber calls 'data nationalism': trying to have data value-add companies 'at home' and to stop the new oil to flow abroad for the extraction of surplus (i.e., through data localisation laws or provisions within law). He suggests though a sort of new digital import substitution strategy is possibly the only alternative for a mid-sized country that is currently in a peripheric position (i.e. exporting raw data and importing data-driven finished products and services). The analysis is a warning for Europe that oligopolistic access to valuable user data by few (US and Chinese) companies forms a barrier to European innovation (white paper OPF, 2019) and economic growth. The more data non-EU firms absorb, the faster the improvement in their algorithms that transform raw materials into value-add data products. The better the data products, the higher the penetration of those products into markets around the world. And since data products generate more data than they use, the greater the data imbalance would become over time.

Already in 2017 it was argued that tech giants are posing a threat as a result of the enormous power they derive from controlling the data, which changes the nature of competition (*The Economist*, 2017). They can anticipate trends and, thus, acquire new companies that may disrupt them, as in the case of Facebook's purchase of WhatsApp. At that time *The Economist* proposed various new measures not falling into traditional anti-trust intervention, such as: considering companies' data assets when assessing merger requests and the price as signal of incumbent buying an emerging threat, identifying colluding algorithms, and giving more control on data to those supplying them. Competition regulation in the context of the digital transformation and with specific respect to online platforms requires a radical renewal of a regulatory regime that was developed for the industrial era and as such is no longer appropriate or useful (Cohen, 2016). Concerning data governance, we can see three specific regulatory approaches in addition to those made on infrastructures above.

First, interventions aiming at possible decentralised control and data sovereignty for individual citizens. It would require deployment of application ecosystems based on personal data-stores and introduction of expiration dates for exclusive access to some data assets (in a fashion similar to copyright expiration). Possibly different for personal vs non-personal data and varying by sector. This could help companies to engage in data-driven innovation with a lower entry barrier (in terms of access to initial data assets). Regulation can be specifically applied to personal data-stores. Other ways are fostering agreements/standards on the structure of personal data stored and support personal data portability across online platforms

Second, give users control over their data by treating data as labour and creating a new market. This may make data more available for other companies that may train their data analytics system and unleash productivity gains (Arrieta-Ibarra et al., 2018). Note that implementation (i.e. having data to train machine learning systems) is now possibly more important than introducing new analytics innovation. The more data to learn AI systems, the more productivity of the system. Data as Labour may also help offset current concerns about AI reducing employment and worsening income distribution.

Third, bring 'algorithmic governance' through application of a few key articles of GDPR. A pragmatic proposal could be to require provision of counterfactual explanation of algorithmic decision to achieve the same objective of GDPR Article 22 without opening the black box and without imposing too much burden on industry players. Alternatively, regulators may decide to impose algorithmic transparency by law (i.e. full application of Article 22).

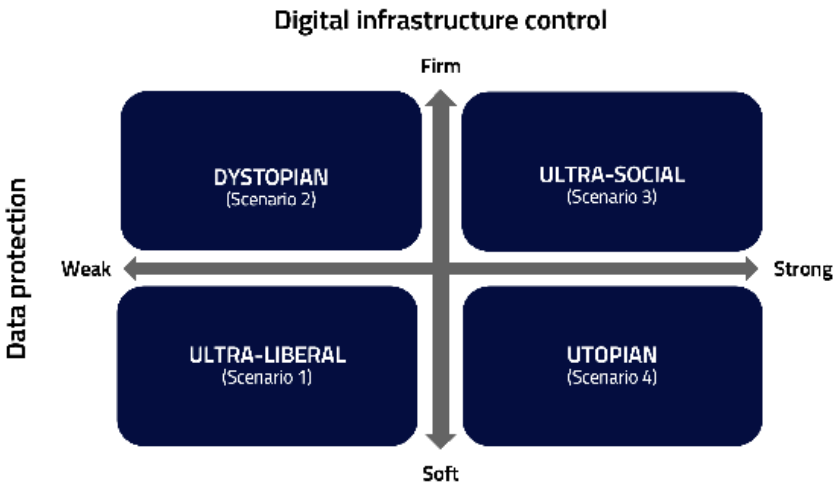
The current digital transformation requires regulatory innovation not only on the 'what' (new rubrics of activities needing regulation) but also on the 'how', meaning entering the domain of algorithmic governance. This requires creation of new institutional mechanisms and technical capacities for defining obligations and overseeing compliance of algorithms. Regulation of current developments is complex and regulators have to catch up. Both in the US and in Europe some initiatives on AI regulation have occurred. For example the 2016 White House report on AI and the Algorithmic Accountability Act directing the FTC with creating detailed policies to ensure oversight for automated decision-making systems. The main focus of the EU guidelines on AI development are set out in EU COM(2018)237 and summarised in a European Parliament briefing document (European Parliament, 2019c) . The GDPR lays down a right for a data subject to receive meaningful information about the logic involved if profiling takes place. However, one can doubt the effectiveness of these actions in light of the above.

SCENARIOS

Scenario construction is an important tool in strategy development in order to explore possible consequences of strategic choices. Scenarios force to focus on the key factors in the strategy and allow to analyse the effects of extreme choices made with respect to these key factors. At the same time scenarios are abstractions and one should realise that the whole collection of factors is more divers. Nevertheless, focussing on the essence and the extreme provides overall guidance for strategic choices, while additional factors have to be taken into account during further refinement.

Digital infrastructures are increasingly considered as critical infrastructures that are vital for the economy. This puts the main policy emphasis on digital infrastructure control. Physical infrastructures like roads, railways, airports, are in Europe often under complete or strong national control. While digital infrastructures are less tangible and are often seamlessly embedded in global infrastructures (like the Internet for example), there is a growing tendency to look into various levels of national control of digital infrastructures. Data is increasingly the engine for value creation and growth in the digital world. This raises issues around ownership, value extraction, privacy, distribution of economic benefits, etc. As a result, the main policy emphasis is on data protection with a focus on data use and user privacy.

As a consequence, the scenarios in this report are derived by building four quadrants from the key axes of infrastructure control and data protection. Scenarios a tool to analyse the effects of extreme choices made with respect to these axes. For the infrastructure control axis, the extreme choices are soft and firm levels of control, while for the data protection axis the extreme choices are weak and strong levels of protection.



Just remind that the scenarios and analysis based on these dominant axes of infrastructure regulation and data protection provide guidance for high-level strategic choices and additional factors should be taken into account during policy development and refinement.

Digital infrastructures control has two extremes. In the upper-level quadrants strong regulatory control or even ownership via a public utility approach lays the focus on the benefits of digital infrastructures for society and citizens, whilst the soft control approach in the lower-level quadrants is hands-off and leaves the development to the free market. While the emphasis is on digital infrastructures such as fixed and mobile networks with currently emerging technologies like 5G and IoT, also software layers such as Software Defined Networks, cloud infrastructures, mobile operating systems, and even platforms are increasingly being considered as digital infrastructure.

Data protection can either be weak with little regulation and as a result data controlled by private market parties and or governments, likely leading to privacy concerns; or strong with regulation addressing topics such as ownership, usage, purpose, and privacy, with the aim to create trust and sovereignty with respect to data, if over-regulated, might lead to hampering innovation. Recent advances in Artificial Intelligence make that also data processing algorithms are increasingly becoming in scope when it comes to data regulation policies. In addition, there are recent developments to also focus on data regulation of machine data, which are an important driver of the Industry 4.0 innovation and may require different regulation than personal data.

The scenarios will be described by considering the position of the key stakeholders, being governments, businesses, citizens and regulators, and analysed with respect to the following key objectives: economic growth, innovation, trust (i.e. from the user perspective), level playing field (i.e. from the supplier perspective) and fairness (i.e. equitable access to economic opportunity).

ULTRA-LIBERAL (1): SOFT INFRASTRUCTURE CONTROL AND WEAK DATA PROTECTION

In this scenario, there are few policies in place, regulators are a small player and governments take a hands-off approach to the infrastructure and there is a lot of freedom in handling data. Businesses that provide infrastructure and services have a lot of room to operate. Citizens will experience little protection and mainly influence by choosing what to use and buy, assuming choice exists. In this scenario business is the strong player.

Deployment of new infrastructure like 5G will be driven by market opportunities mainly, which may result in availability only in densely populated urban areas. Also, IoT and cloud development are left to the market, as well as industry development and standardisation/self-regulation efforts. Cybersecurity would be pursued through co-regulation, self-regulation, and standardisation rather than strict governmental regulation.

Data will to a large extent be controlled by large private enterprises, which continue to extract behavioural surplus without effective oversight and effective sanctions. Online platforms and tech giants can increase their advantages in terms of access to data which in turn enables continuous learning and improvement of their algorithms.

Economic growth in this scenario will be mainly business driven. Infrastructure investments have a multiplier effect on both short- and long-term economic growth. Without active government involvement in driving innovative infrastructure such as 5G, deployment might be delayed due to lack of short-term financial resources or returns. Innovation generally benefits from government stimulation, a hands-off government with respect to infrastructure may lead to less innovation in this scenario. Weak data protection has two sides when it comes to innovation, on the one hand it allows new ways of using data which fuels innovation, while on the other hand it may prevent citizens adopting new technology resulting from privacy concerns for example.

Trust for citizens comes down to trusting governments, business and regulators. Given that this scenario is mainly driven by business, it all depends on the trust citizens have in these businesses. Something that will vary from business to business. Since the government acts hands-off this scenario has a high likelihood of the winner takes it all. Since there is little regulation both on infrastructure and data, dominant market players will have ample possibilities to further strengthen their position. As a result, this scenario will highly unlikely produce a level playing field. Also, fairness is under pressure in this scenario, since the deployment of both infrastructure and services will be mainly market driven, as an example the deployment of 5G may be limited to densely populated urban areas, generating polarisation of access as thus no equitable access to economic opportunity (digital divide).

In this scenario neither Europe's technological sovereignty nor individual data sovereignty for European citizens are likely to emerge. Imbalances in the European data economy (export raw data, import refined results) will likely not be removed, and guidelines about data processing and ownership most likely remain without tangible results.

DYSTOPIAN (2): FIRM INFRASTRUCTURE CONTROL AND WEAK DATA PROTECTION

In this scenario, governments control the infrastructure while there is freedom in handling data. The role of the regulator

depends on the government approach of either strong regulatory control or public utility ownership. Businesses that provide infrastructure will face government intervention either directly or via strong government-controlled regulator. Businesses that provide data driven services have more room to operate but nevertheless can expect government interference due to the fact that the data travels over government-controlled infrastructures. Citizens will experience that access to, and use of, infrastructure and to a lesser extent services and platforms is directly or indirectly controlled by governments. In this scenario government is the strong player.

Deployment of new infrastructure like 5G, IoT and cloud will be driven by governments taking into account economic development and geopolitical development. As a result, governments may choose to work closely with a limited set of trusted infrastructure providers. Infrastructure cybersecurity will be pursued through strict governmental regulation.

Lack of data protection and strong government control over the infrastructure also gives governments ample opportunities to control the data, either directly or through private enterprises. Online platforms and tech giants can only increase their advantages in terms of access to data with government (in)direct consent. Imbalances in the European data economy (export raw data, import refined results) will likely not be removed.

Economic growth in this scenario will be mainly driven by government and selected businesses. Active government involvement in driving deployment of innovative infrastructure will boost global economic competitiveness. Innovation generally benefits from government stimulation, but at same time requires freedom for experimentation and alternatives. Too much government control may lead to less innovation in this scenario.

In this scenario, trust from a user perspective is mostly relying on trust in the government. Since the government and government-selected businesses are dominant this scenario will not produce a level playing field. Fairness is determined by the government in this scenario, since the deployment of both infrastructure and services will be mainly government driven.

This scenario with strong government intervention and without personal data protection is considered so much inconsistent with the European values, that it is not a viable option for Europe.

ULTRA-SOCIAL (3): FIRM INFRASTRUCTURE CONTROL AND STRONG DATA PROTECTION

This scenario combines governments control over the infrastructure with strong data protection. Given that regulation originates from parliament in democracies and is controlled by the regulator, the regulator plays an important role in this scenario with strong data protection regulation. It is also likely in this scenario that governments exert their infrastructure control mostly via strong regulatory control rather than full public utility ownership, which further strengthens the role of the regulator. Businesses that provide infrastructure will face government intervention via an empowered regulator. Businesses that provide data driven services can expect regulator interference. Citizens will experience a mix of government control and regulator interference, where the regulator safeguards data protection of citizens also towards governments. In this scenario the regulator is the strong player.

With respect to the digital infrastructures, the combination of firm government control and strong data protection could lead to public private partnerships for higher level infrastructure layers like clouds and platforms. The public sector would invest to overcome the barrier of high capex and to safeguard inclusion. Examples might be health or education cloud platforms deployed on top of a combination of fixed, 5G and IoT networks. To encourage private co-investment, the policy chosen could call for a lower

intensity regulation. Such a policy could nonetheless include new rules and decisions on digital competition policy (monitoring of anti-competitive mergers, considering price and data assets, new definition of market power, auditing collusive algorithms, etc.). In addition to direct regulatory action, the government as a user and provider of digital infrastructures could establish good practices in data exploitation.

In this scenario data protection regulations such as GDPR should be fully implemented and new measures and policy actions for individual data (both raw and behavioural), rights to be forgotten, to withdraw consent, and to explanation, with algorithm transparency being mandatory and legally binding. An identity system would be guaranteed by law and regulation and made possible through the adoption of (sovereign) eID solutions.

Economic growth in this scenario will be mainly driven by public-private partnerships. Active government involvement in driving deployment of innovative infrastructure will boost global economic competitiveness. Innovation benefits from government stimulation and public private partnerships. Strong data protection has again two sides when it comes to innovation, on the one hand it restricts new ways of using data which hinders innovation, while on the other hand it may take away concerns from citizens in adopting new technology.

In this scenario, trust from a user perspective is mostly relying on trust in the regulator. The independent position of regulators in democracies and the fact that regulators also protect citizens interests, should increase trust in digital. Since the government is firmly controlling the infrastructure it may not be a full level playing field. Regarding data-driven services the likelihood of a level playing field is higher given the regulator ability to safeguard data protection and act against dominance. Fairness is determined by the regulator and to a lesser extent by the government in this scenario.

In principle, this scenario would allow for strengthening both Europe's technological sovereignty and individual data sovereignty for European citizens in a world without regulatory frictions and unintended effects.

UTOPIAN (4): SOFT INFRASTRUCTURE CONTROL AND STRONG DATA PROTECTION

In this scenario, governments take a hands-off approach to the infrastructure, while there is a strong data protection. Businesses that provide infrastructure have a lot of room to operate. Citizens experience data protection and can influence success of business by choosing what to use and buy, while their interests are safeguarded by the regulator. In this scenario citizens are the strong player.

Infrastructure development and deployment will be market driven with governments staying at arm's length. A more open playing field for data-driven service providers may lead to accelerated infrastructure deployment due to larger demand and faster uptake of services by users.

Data protection will safeguard citizens interests and the combination of freedom to operate on the infrastructure side may turn out to be a fertile environment for the development and deployment of trusted data-driven services.

Economic growth in this scenario will be mainly driven by a combination of technology push by businesses and market pull by citizens willing to explore and use trusted services. Innovation in this scenario will be driven by ecosystems that bring together businesses, innovators, entrepreneurs and early adopter citizens,

but the business environment will show uncertainties by lack of regulation.

In this scenario, trust from a user perspective is mostly relying on the combination of the regulator and the diversity of businesses due to the lack of dominant market players. Since the citizens, supported by the regulator, are the key actors in this scenario it is likely to produce a level playing field for data use, but not necessarily for commercially driven infrastructure. Fairness is determined by the regulator in this scenario, and to a certain extent to the citizens preferences.

In this scenario individual data sovereignty for European citizens is likely to emerge. It is also possible to achieve Europe's technological sovereignty, although this will not come as long as digital infrastructures are not regulated and incumbent tech giants are left untouched, since regulatory intervention needs real levers in the absence of any form of regulation of digital infrastructures.

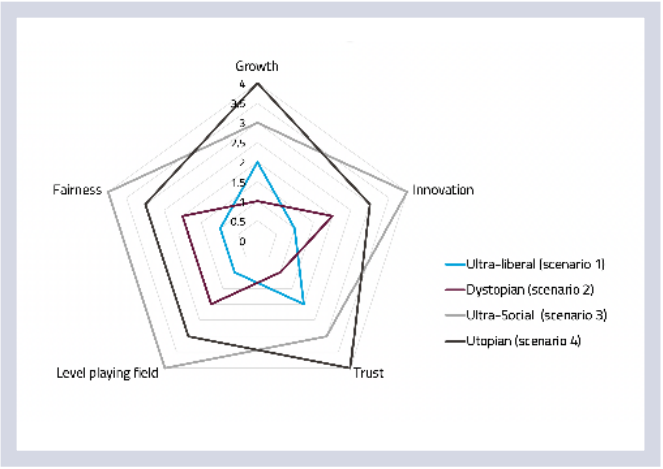
IMPACT ASSESSMENT ON POLICY OBJECTIVES

The scenarios contain a qualitative assessment of their likely impact on the five policy objectives: economic growth, innovation, trust (i.e. from the user perspective), level playing field (i.e. from the supplier perspective) and fairness (i.e. equitable access to economic opportunity).

Based on the qualitative assessments per scenario, for each policy objective the scenarios have been placed in the strict order from least (1) to most impact (4), thus providing a relative comparison between the scenarios. This has been depicted in the spider diagram. Note that using a strict order forces a strong discrimination between the scenarios and leaves less room for nuances. The spider diagram therefore magnifies differences and has to be seen as a tool to give a quick insight into the relative strengths and weaknesses of the scenarios, rather than absolute differences.

The impact assessment shows that the ultra-social and utopian scenarios are very similar and deliver the most balanced overall result. The ultra-social scenario delivers somewhat better on fairness and level playing field due to the strong role of the regulator in that scenario. Also, the government hands-on attitude is assumed to be translated in relatively high public investments in research and innovation.

Both Scenarios 1 and 2 suffer in particular of lack of fairness, level playing field and trust that has also negative effects on growth and innovation. Moreover, public Investments in infrastructure (missing in scenario 1) have a multiplier effect on both short- and long-term economic growth. In scenario 2 the state holds business in check, hampering also innovation. The investments in infrastructure have first order effects that should be stronger than the indirect effects from more innovation (i.e. Scenario 1) and from leaving the growth and innovation to tech giants.



Finally, it should be noted that these scenarios consider the more extreme choices, while in reality one finds mixed approaches that combine measures from different scenarios.

EUROPEAN DIGITAL SOVEREIGNTY – CONCLUSIONS AND RECOMMENDATIONS

As stated, the European struggle with COVID-19 contact tracing apps has once more illustrated the importance of European digital sovereignty. The objective of this report is to provide a concise scenario-based framework together with an impact analysis as an instrument for the development of a policy strategy to achieve such sovereignty. Given the current state of affairs and the different views on the complex task of developing policies with many stakeholders and many different interests, bringing the key ingredients together in an orderly and concise framework is urgently needed.

There is currently a vicious cycle in which a very small number of (non-EU) companies have oligopolistic access to valuable user data. The more data they access, the faster the improvement of their algorithms that create value added products from these data, the higher the penetration of these products into world markets and the greater the generation of new valuable data that feed the cycle. This cycle forms a barrier to European innovation and growth, constitutes a serious threat to European sovereignty and needs to be slowed down and eventually broken via novel, agile regulatory tools.

The analysis shows that long term consistent growth is best achieved in scenarios where interests of the various stakeholders are balanced, and the rights of citizens and businesses are protected through a combination of regulation and dynamic interaction of the stakeholders. Infrastructure control is either hands-off or implemented via regulation rather than ownership. Data ownership and access control is implemented through data governance policies concerning both private and industrial data.

Europe, through coordinated action between the European Commission and the Member States, is called upon to use this framework to virtuously connect *makers* (industry) and *shapers* (authorities, citizens) in order to create a sovereign European digital reality with innovation enhancing regulation that respects European values and rights while creating equal economic opportunity for all actors. A dynamic, balanced and proportionate regulatory approach is required to strive towards optimal conditions for innovation with equitable access to economic opportunity in a trusted digital world. Such an approach will create a more level playing field that enables new industry players (including European) to enter and diminish the dependency of citizens and governments on oligopolistic industry actors.

REFERENCES

Aggarwal, V., & Reddie, A. (2018a). Comparative industrial policy and cybersecurity: a framework for analysis. Journal of Cyber Policy, 3(3), 291-305. (In note 21).

Albrycht, I., & Swiatkowska, J. (2019). The Future of 5G or Quo Vadis, Europe? Krakow: the Kosciuszko Institute Policy Brief. Retrieved from https://ik.org.pl/wpcontent/uploads/ik_policy_brief_5g_eng.pdf.

Arrieta-Ibarra, I., Goff, L., Jiménez-Hernández, D., Lanier, J., & Weyl, E. (2018). Should We Treat Data as Labor? Moving beyond «Free». AEA Papers and Proceedings, American Economic Association, 108, 38-42.

BMWi. (2019). Project GAIA-X. A Federated Data Infrastructure as the Cradle of a Vibrant European ecosystem Berlin: Federal Ministry for Economic Affairs and Energy. BMWi, retrieved from: https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.pdf?__blob=publicationFile&v=4, 22/11/2019.

Brynjolfsson, E., Collis, A., & Eggers, F. (2019). Using massive online choice experiments to measure changes in well-being. Proceedings of the National Academy of Sciences, 116(15), 7250.

Buiten, M. C. (2019). Towards Intelligent Regulation of Artificial Intelligence. European Journal of Risk Regulation, 10(1), 41-59.

Campbell, K., Diffley, J., Flanagan, B., Morelli, B., O'Neil, B., & Sideco, F. (2017). The 5G Economy. HIS, retrieved from: https://cdn.ihs.com/www/pdf/IHS-Technology-5G-Economic-Impact-Study.pdf, 20/11/2019.

Cheung, T. (2018). The Rise of China as a Cybersecurity Industrial Power: Balancing Between National Security, Geo-Political, and Development Priorities. Journal of Cyber Policy, 3(3), 306-326.

Codagnone, C. (2017). Lobbying as Rhetorical Framing in the "Sharing Economy»: a Case Study on the Limits and Crisis of the Evidence Based Policy Paradigm. DigiWorld Economic Journal(108), 15-43.

Codagnone, C., Karatzogianni, A., & Matthews, J. (2018). Platform Economics: Rhetoric and Reality in the 'Sharing Economy': Emerald Publishing Limited.

Cohen, J. (2012). Configuring the networked self. New Haven, CT: Yale University Press.

Cohen, J. (2015). Studying law studying surveillance. Surveillance & Society, 13, 191-201.

Cohen, J. (2016). The Regulatory State in the Information Age. Theoretical Inquiries in Law, 17, 369 414.

Cohen, J. (2019). Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford: Oxford Unibversity Press.

CSIS. (2014). Net Losses: Estimating the Global Cost of Cybercrime. Washington, D.C.: Center for Strategic and International Study (CSIS).

Deloitte. (2017). Guiding the IoT to safety. The Internet of Things and the role of government as both user and regulator. Deloitte, retrieved from: https://www2.deloitte.com/content/dam/insights/us/articles/3612_Guiding-IoT-to-safety/DUP_Guiding-the-IoT-to-safety.pdf, 21/11/2019.

Domingos, P. (2012). A few useful things to know about machine learning. Commun. ACM, 55(10), 78-87.

Ethics Advisory Group. (2018). Towards a Digital Ethics. Brussels: European Data Protection Supervisor (EDPS), Retrieved from: https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf, 16/10/2019.

European Parliament. (2019a). Cybersecurity of critical energy infrastructure. Brussels: European Parliament. Retrieved from: https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642274/EPRS_BRI(2019)642274_EN.pdf , 21/11/2019.

European Parliament. (2019b). Economic impacts of artificial intelligence (AI). Briefing. Brussels: European Parliament. Retrieved from: http://www.europarl.europa.eu/RegData/etudesBRIE/2019/637967/EPRS_BRI(2019)637967_EN.pdf ,19/10/2019.

European Parliament. (2019c). EU guidelines on ethics in artificial intelligence: Context and implementation. Briefing. Brussels: European Parliament (retrieved from: https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf ,21/11/2019).

European Parliament and Council. (2017). Joint Communication of the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. JOIN(2017) 450 final, Brussels: European Parliament and Council.

Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a 'right to explanation. AI Magazine, 38(3), 50-57., 38(3), 50-57.

ITU. (2018). Setting the Scene for 5G: Opportunities & Challenges Geneva: International Teleccommunication Union (ITU), retrieved from: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.5G_01-2018-PDF-E.pdf , 21/11/2019.

Lee, K. (2018). AI Superpowers: China, Silicon Valley and the New World Orde. New York, NY: Houghton Mifflin Harcourt.

Lee, S., Zhu, L., & Ross, J. (2017). Data Governance for Platform Ecosystems: Critical Factors and the State of Practice. Paper presented at the Twenty First Pacific Asia Conference on Information Systems, Langkawi.

Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development. Journal of Global Information Technology Management, 22(1).

Mazzucato, M. (2015). The Entrepreneurial State: Debunking Public vs. Private Sector Myths. London: Anthem Press. Morgan, S. (2015, December 20). Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020. Forbes.

NIS Cooperation Group. (2019). EU Coordinated Risk Assessment of the Cybersecurity of 5G networks. Brussels: European Commission.

O'Hara, K. and Hall, W. (2018) Four internets: the geopolitics of digital governance.

Olhede, S., & Wolfe, P. (2017). When algorithms go wrong, who is liable? Significance, 14(6), 8-9.

OPF (2019). Ocean Protocol: A decentralised substrate for AI data and services. Tehnical White Paper. Singapore: Ocean Protocol Foundation (OPF), retrieved from: https://oceanprotocol.com/tech-whitepaper.pdf , 18/10/2019.

Palovirta, M., & Grassia, P. (2019). A case for a European strategy on tech leadership. Politico. Retrieved from https://www.politico.eu/sponsored-content/a-case-for-a-european-strategy-on-tech-leadership/, 19/11/2019.

Polanyi, K. (1957). The Great Transformation: The Political and Economic Origins of Our Time. Boston: Beacon Press.

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. Journal of Cybersecurity, 4(1), tyy001.

Solove, D. (2013). Privacy self management and the consent dilemma. Harvard Law Review, 126, 1880–1893. Susarla, A. (2018, August 17). Facebook shifting from open platform to public utility. Retrieved from https://www.upi.com/Top_News/Voices/2018/08/17/Facebook-shifting-from-open-platform-to-public-utility/1721534507642/ , 20/11/2019.

The Economist. (2017, May 6). The world's most valuable resource is no longer oil, but data; The data economy demands a new approach to antitrust rules. The Economist.

Timmers, P. (2018). The European Union's cybersecurity industrial policy. Journal of Cyber Policy, 3(3),

United Nations. (2019). The age of digital interdependence. Report of the UN Secretary-General's High-level Panel on Digital Cooperation. New York: United Nations. Retrieved from: https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf , 21/11/2019.

Wachter, S., Mittelstadt, B., & Russell, C. (2018). Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR. Harvard Journal of Law & Technology, 31(2), 841-887.

Walport, M. (2014). The Internet of Things: making the most of the Second Digital Revolution, a report by the UK Government Chief Scientific Adviser. London: UK Government Office for Science (retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf, 21/11/2019).

Weber, S. (2017). Data, development, and growth. . Business and Politics, 19(3), 397-423.

World Economic Forum. (2014). Delivering Digital Infrastructure. Advancing the Internet Economy. retrieved from: http://www3.weforum.org/docs/WEF_TC_DeliveringDigitalInfrastructure_InternetEconomy_Report_2014.pdf, 15/10/2019.

Yeung, K. (2017). 'Hypernudge': Big Data as a mode of regulation by design. Information, Communication & Society, 20(1), 118-136.

Zuboff, S. (2019). The Age of Surveillance Capitalism. London: Profile Books Ltd.

ACKNOWLEDGEMENTS

In the context of its activities in strategic innovation of Europe, EIT Digital decided to launch a study focusing on the main policy challenges emanating from the need for European sovereignty concerning digital infrastructures and the handling of data. The study followed a scenario-based approach to structure and assess the potential impact of policy measures with the main focus on Digital infrastructure control and regulation and data protection. Digital Enlightenment Forum was contracted to execute the study under the guidance of EIT Digital senior staff.

We acknowledge the contributions of Digital Enlightenment Forum for providing the breadth and depth of this study via interdisciplinary stakeholder discussions as well as an extensive literature survey. A special thanks to Jacques Bus, George Metakides, Paul Timmers of Digital Enlightenment Forum, to Cristiano Codagnone of the University degli Studi di Milano and Thanassis Tiropanis of University Southampton for their support in managing and creating this in-depth study.

This document is built on the report 'European Digital Infrastucture and Data Sovereignty – Full Report' (ISBN 978-91-87253-62-1). Download a free copy at: www.eitdigital.eu/newsroom/publications.

Publisher
EIT Digital
Rue Guimard 7
1040 Brussels
Belgium
www.eitdigital.eu

Contact
info@eitdigital.eu

EIT Digital is supported by EIT,
a body of the European Union

ISBN 978-91-87253-62-1