A DIGITAL UNION BASED ON EUROPEAN VALUES

FEPS
FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES

IVANA BARTOLETTI

FEPS
Primer Series

A DIGITAL UNION BASED ON EUROPEAN VALUES

Ivana Bartoletti

A DIGITAL UNION BASED ON EUROPEAN VALUES

The need to balance economic and social integration

FEPS
Primer Series

DIETZ

This book has been produced with the financial support of the European Parliament.

Bibliographical information of the German National Library
The German Library catalogues this publication in the German National Bibliography; detailed bibliographic information can be found on the internet at: *http://dnb.dnb.de*.

ISBN 978-3-8012-3108-8

FEPS Editors: L. Andor, A. Skrzypek
FEPS Project Coordinator: E. Gil, C. Reder
FEPS Expert Review: G. Rinse Oosterwijk

Published by
Verlag J.H.W. Dietz Nachf. GmbH
Dreizehnmorgenweg 24, D-53175 Bonn

Published in association with the
Foundation for European Progressive Studies
www.feps-europe.eu
European Political Foundation – N° 4 BE 896.230.213

FEPS
Primer Series

– Vol. 5

Cover design and typesetting: Rohtext, Bonn
Cover picture: Shutterstock / greenbutterfly
Printing and processing: Bookpress, Olsztyn

Printed in Poland 2024

Find us on the internet: *www.dietz-verlag.de*

Contents

Foreword

The digital transition will significantly affect the work, education and social life of all Europeans. Digitalisation impacts public service delivery and, through social media, even affects our democratic processes.

Europe currently lies between a rock and a hard place regarding the digital industrial revolution. Silicon Valley-based Big Tech platforms dominate the European market, pursuing their particular brand of data capitalism, while the Chinese model represents a dystopian version of the digital surveillance state. The challenge is to align our European digitalisation model with the social market economy, vital public services and a robust civil society.

The EU is a technology taker, but it has become the global technology regulator. Over recent years, European policymakers have proposed a whole raft (and a veritable alphabet soup) of digital laws – GDPR, DMA, DSA, DGA, AIA, you name it – to obtain more transparency and accountability from the dominant tech firms and the digital infrastructures they control. These laws are also aimed at countering monopolistic power over digital market spaces and the polarising effects of social media on democratic processes. This proactive agenda is shaping tech policy around the world.

But is it enough to bring us to a human and society-centric tech ecosystem, especially with developments such as artificial intelligence (AI) applications inundating us? This primer is meant to provide the reader with a grounded understanding of the technology and policy relevance of the developments that have been taking place and are expected to shape the debate in the coming years. We also aim to raise some thought-provoking ideas on what needs to be done to help European tech policy establish itself on firm foundations and foster a progressive vision of society.

This agenda cannot only be defensive and we cannot look to Big Tech for technological fixes to solve such problems as poverty, poor

public health and failing education. While those problems are as acute as ever, there is one immediate challenge that we need to address: our public institutions and how we work and live are being reshaped to serve Big Tech's profitmaking and power. Therefore we must develop an alternative vision and programme for digital tech that aligns with European values.

Gerard Rinse Oosterwijk
FEPS Digital Policy Analyst

Introduction

Technology continues to evolve very quickly, crossing frontiers and changing the way people live their lives. Our society is run on code: whether we are seeing our doctors, using our phones or paying our taxes, we are almost constantly interacting with software and algorithms. And technology, data, AI and 5G have all left the technology corner to become the flesh and bones of mainstream domestic politics, geopolitics and diplomacy.

In recent years, the European Union has dived into the digital diplomacy landscape. Its strategy for competing with other global giants is demonstrated by the so-called 'Brussels effect', namely the EU's ability to act as a super regulatory power through its broad influence. The size and nature of the EU legislative process, within the framework of which 27 Member States can negotiate and share such a large market brings enviable leverage. Recently, a lot of effort has gone into making the most of this power by ensuring that data collected in Europe benefits European citizens and businesses, and fosters economic growth.

Europe's response to the colossal events of the Covid-19 pandemic and then the war in Ukraine has accelerated the pursuit of digital and technological sovereignty and reinvigorated alliances in the digital realm.

The purpose of this primer is threefold. First, to create a shared understanding of the evolution of the digital ecosystem from the internet to decentralisation, and to fully comprehend the changes that foundational models are bringing into our world.

Second, to appreciate the full range of activities undertaken by the EU, aimed at giving structure to the EU's ambition to achieve technological sovereignty.

Third, we will face the problem that, despite all its ambition, Europe is still lagging behind in technology. Sovereignty, conceived here as Europe's ability to stand tall in a complex global supply

chain, requires a multi-layered approach, the creation of internal demand, a new role for government and a determination to digitise public services.

There is no easy recipe for growth, but one thing is certain: growth must combine innovation, productivity and respect for human dignity. We cannot call it progress if we manage to obtain the first two at the expense of the last.

PART I: Setting the stage

The internet

The internet is often cited as our era's greatest innovation, and indeed it is almost impossible to envisage life without it. It has reshaped the way we engage with others globally and its many applications (apps) aid us in our daily routines. But what exactly is the internet?

The internet is a vast network connecting computers all over the world through approximately 1,200,000 kilometres of cables, both underwater and underground. Each cable carries glass fibres that transmit data in the form of light pulses. To protect these fibres from corrosion and shark attacks, they are wrapped in layers of insulation and buried under the seabed using specialised ships. When anyone accesses the internet, data is transmitted via these cables, requesting access to data stored on other machines. When accessing the internet, most people use the world wide web.

Most computers are connected to the internet with no need for wires, utilising wi-fi and a modem linked to a socket. The modem is then connected to an external box through wires, which are then routed to a series of cables located underground. In combination, these cables function to convert radio waves into electrical signals to fibre optic pulses, and vice versa.

Routers (also known as junction boxes) are located at every connection point in the underground network. Their primary responsibility is to determine the optimum pathway for transferring data from the user's computer to the computer they intend to connect with.

The internet transmits data worldwide, crossing over land and sea. Network providers communicate with each other until the data

reaches its nearest endpoint. After this, it passes through local routers until it reaches the computer with the matching IP address.

Computer systems can communicate on the basis of a set of guidelines known as the Transmission Control Protocol (TCP) and the Internet Protocol (IP). This is somewhat similar in functionality to the postal service. Information is sorted and packaged into a standardised envelope that must include the sender's details, the recipient's details and the contents of the envelope. IP explains how the addressing system used for data transmission works, while TCP provides instructions on how to organise and transmit data.

Turning to internet speed, bandwidth determines how much data can be downloaded per second. For browsing the internet, checking emails and updating social media accounts, a speed of 25 megabits per second is typically sufficient, but streaming 4k movies, playing online video games or live streaming may require speeds of 100–200 megabits per second. The quality of the underground cables linking users to the rest of the world significantly influences download speeds. Fibre optic cables transmit data at a much higher rate than their copper counterparts, and the speed of the home internet is often affected by the infrastructure available within the local region.

The World Wide Web: from websites to decentralisation

The internet is a globally connected network that has evolved over time, revolutionising the ways we communicate, consume information and conduct business. Its history dates back to the early 1960s, when it was originally known as ARPANET, a project funded by the United States Department of Defence.

However, it wasn't until Tim Berners-Lee designed the World Wide Web in the 1990s that the internet as we know it today truly began to take shape. The web allowed for the easy sharing of information and the creation of user-friendly interfaces that could be accessed by anyone with an internet connection.

THE TECHNOLOGY EXPLAINED:
the birth of the World Wide Web in a nutshell

Tim Berners-Lee, while at the European Organization for Nuclear Research (better known as CERN), hatched a plan for an open computer network to keep track of research at the particle physics laboratory located in the suburbs of Geneva, Switzerland. Berners-Lee's modestly titled 'Information Management: A Proposal', which he submitted to obtain a CERN grant, would become the blueprint for the World Wide Web.

But in thinking about the problem of incompatibility, he realised that it would be even better if visiting scientists, after they returned to their home labs, could still share their data, regardless of where they were based.

Berners-Lee also created the three main innovations that go hand in hand with the WWW: HTTP (hypertext transfer protocol), URLs (universal resource locators, which were originally known as URIs or universal resource indicators), and HTML (hypertext markup language). HTTP allows you to click on a link and be brought to that document or Web page. URLs serve as an address for finding a document or page. And HTML gives you the ability to put links in documents and pages so they connect with one another.

What is Tim Berners Lee doing now? Tim founded the Web Foundation with the aim of ensuring that the web works for everyone. His advocacy efforts focus on equal access, digital literacy and, most pertinent to this primer, the 'weaponisation' of the web, made possible by the concentration of power among a handful of companies.

The rise of internet service providers (ISPs), the introduction of dial-up and the development of search engines were pivotal moments in the mainstream adoption of the internet. ISPs enabled individuals and businesses to connect to the internet through paid subscriptions and paved the way for faster, more reliable connections. Dial-up al-

lowed users to connect to the internet through phone lines, albeit at a much slower speed.

The development of search engines such as Yahoo! and Google made it easier for users to navigate the vast amount of information available on the internet. Before search engines, users had to know the exact URL or rely on directories to find what they were looking for.

From Amazon to eBay, online shopping quickly became the way of the future, with online payment processing quickly becoming a cornerstone of e-commerce. Today, the world of e-commerce continues to evolve. From virtual storefronts to mobile apps, there are so many convenient ways to shop online.

Over the past two decades, social media has transformed the way people interact with each other online. Platforms such as Facebook, X (formerly Twitter), Instagram, YouTube and Snapchat have unique features that have revolutionised communication, content sharing, and information consumption. Facebook has become the world's largest social network, X (Twitter) is known for its bite-sized updates on every topic under the sun, Instagram has had a massive impact on visual storytelling, YouTube has revolutionised the way we consume video content, and Snapchat introduced the concept of disappearing messages. Each platform has had its own unique impact and has contributed to the ever-evolving social media landscape.

Online shopping and social media have profoundly changed the way we organise our life, connect and share our lives online. But what has changed our lives most dramatically is the mobile internet or smartphone. The first smartphone, IBM Simon, was launched as early as 1993, but it was the iPhone that revolutionised the mobile industry. Today, more people browse the internet on their mobile devices than on desktop computers.

The mobile internet era has also brought forth the emergence of mobile apps. From social media to gaming, there seems to be an app for everything. The rise of app stores and the app economy has provided developers with a new platform on which to innovate and (hopefully) prosper. Mobile app revenue has now surpassed that of PC and console games combined. The mobile internet has opened

up a world of possibilities, and it continues to shape the future of the internet.

The so-called Internet of Things (IoT) is now taking over many of the tools that we use in daily life, with everything from cars to fridges being connected to the internet. It's a world in which machines 'talk' to each other, and (potentially) decisions are made without human intervention. Augmented Reality (AR) and Virtual Reality (VR) are also set to change the game. They offer a new way of experiencing the internet, transforming how we shop, play and learn. Blockchain technology is yet another game-changer. It offers a new way of ensuring trust online, and it's being used in everything from cryptocurrencies to online voting.

THE TECHNOLOGY EXPLAINED: The Internet of Things

The Internet of Things (IoT) refers to a network of interconnected devices that communicate with other IoT devices and the cloud. These devices can be mechanical or digital machines, consumer objects, or even living beings, such as a person with a heart monitor implant or a farm animal with a biochip transponder. IoT devices have embedded technology, including sensors and software, which allows them to collect and transfer data without human intervention.

IoT is increasingly being used by organisations in various industries to increase efficiency, provide better customer service, make data-driven decisions, and add value to their businesses. The system allows for seamless data transfer without requiring any human-to-human or human-to-computer interactions.

An IoT ecosystem consists of smart devices that are web-enabled and equipped with embedded systems, such as processors, sensors and communication hardware. These devices collect, send and act on the data they obtain from their surroundings. As a result, IoT has immense potential for transforming the way we live and work, and it offers an exciting glimpse into the future of technology.

However, the IoT raises a number of questions, especially in relation to privacy. IoT tools are becoming increasingly prevalent because of their convenience, but with that convenience we are witnessing an increase in privacy infringements. IoT tools and smart applications collect a large amount of data, including recordings, movements and interaction metadata from which it is possible to obtain very sensitive information about users, including psychological traits, states of mind, interests and concerns. In addition to privacy considerations, the key issue that will have to be discussed moving forward is the purpose of IoT data extraction. Data is extremely valuable, but the benefits of its extraction are not equally distributed: large tech companies reap most of the dividends.

THE TECHNOLOGY EXPLAINED: augmented and virtual reality

Augmented Reality (AR) is a technology that adds digital elements to the real world, often by using the camera on a smartphone. AR components blend into a person's perception of the real world, thus enhancing both it and the virtual world. Pokémon Go is a popular AR technology that allows players to locate and capture Pokémon characters that appear in the real world. AR's primary value is its integration of sensations, perceived as natural parts of an environment. One of AR's advantages over VR is that it can be accessed with just a smartphone.

Virtual Reality (VR) is a simulated experience in which the world you're standing in is replaced with a virtual one. This can be done with something as simple as a plastic holder you put your phone into, but most people prefer head-mounted displays these days. VR has revolutionised gaming and entertainment by allowing users to immerse themselves in a highly simulated environment. It is also a big player in medical or military training and business (for example, virtual meetings). VR has the advantage over AR as it creates a completely virtual reality experience.

What is the difference? AR and VR differ significantly in terms of reality alteration. AR adds digital elements to the real world, while VR replaces the real world with a simulated one. User control differs as AR users can control their presence in the real world, while VR users are controlled by the system. AR can be accessed with just a smartphone, while VR requires a headset device. Both have different industry applications, with AR commonly used in training, education, audits, and inspections, and VR in gaming, entertainment, medical and military training, and virtual meetings.

The Fourth Revolution

We now live in what is often called the Fourth Industrial Revolution, or Industry 4.0. This is deemed to be the latest phase in the progression of human civilisation. It refers to the current and developing environment in which self-styled 'disruptive' technologies and trends, such as the Internet of Things (IoT), robotics, virtual reality (VR), and artificial intelligence (AI), are changing the way we live and work.

The Fourth Revolution builds on the Third Industrial Revolution, or the Digital Revolution, which began in the mid-twentieth century. That was marked by the transition from mechanical and analogue electronic technology to digital electronics and the birth of information technology and the internet. The Fourth Revolution, however, goes beyond simple digitalisation. It represents new ways in which technology is becoming embedded within societies and even within the human body. This revolution is characterised by a fusion of technologies that is blurring the lines between the physical, digital and biological spheres.

The Fourth Revolution is transforming industries and economies through smart and autonomous systems fuelled by data and machine learning. It is producing new types of products and services and transforming operational models. The scope of these changes and the speed at which they are occurring are the fundamental differences between the Fourth Revolution and its predecessors.

The 'Industrial Revolution' typically refers to the first significant period of industrialisation in the late eighteenth and early nineteenth centuries, which fundamentally changed agriculture, manufacturing, mining and transportation. This change was facilitated largely by steam power, the development of machine tools and the rise of the factory system.

The Fourth Revolution, however, is fundamentally different. First, the speed of change is exponentially faster because of the networked nature of digital communication and decision-making. Second, the scope of this revolution is broader, touching almost every industry in every country. Third, the systemic impact of the Fourth Revolution has the potential to transform entire systems of production, management and governance. Fourth, it involves the transformation of entire systems, across (and within) countries, companies, industries and society.

In a nutshell, the original industrial revolution was propelled by steam; electricity fuelled the second; the third was driven by initial automation and machinery; and the fourth industrial revolution is being moulded by cyber-physical systems or smart computers,

These changes are affecting our lives significantly, in many ways. At the societal level, it is changing how we communicate, learn, entertain ourselves and interact with each other. On the personal level, it is changing aspects of everything from our health to our work and shopping habits.

In terms of work, the Fourth Revolution is creating new jobs, while rendering others obsolete, leading to significant labour market shifts. It also makes possible remote working and more flexible, digitally-connected workplaces. In health care, advances in genetics, AI and bioengineering are opening up new possibilities for personalised medicine and longevity. In education, the digital transformation makes possible new learning methods, with personalised and remote learning opportunities.

The Fourth Revolution also raises significant questions about privacy and security. The vast amount of data collected and processed in our interconnected world presents significant privacy concerns.

Similarly, the proliferation of digital technologies also heightens our vulnerability to cyber attacks.

While the Fourth Revolution has the potential to raise global income levels and improve the quality of life for populations around the world, it also has the potential to exacerbate social inequalities and disrupt labour markets. As the reliance on technology increases, ensuring equal opportunity and access becomes a growing concern.

To more fully understand where we are now, therefore, we need to look at the various components of the Fourth Revolution. In a nutshell, it involves a shift from the age of machinery and mass production to an age of smart systems and digitalisation. This shift is impacting every facet of life and demands the constant development of new policies and new forms of governance.

The impact of artificial intelligence

The term 'artificial intelligence' was originally proposed and put into circulation by John McCarthy in the process of organising a scientific gathering at Dartmouth College in the summer of 1956.[1] The term gained traction immediately. Despite its success, however, what 'AI' really designates has remained rather murky and highly contentious. 'AI people', as Robert Schank wrote famously in 1990, 'are fond of talking about intelligent machines, but when it comes down to it, there is little agreement on exactly what constitutes intelligence. And, it thus follows, there is very little agreement in AI about exactly what AI is and what it should be.'[2]

Agreeing on how we define artificial intelligence is critical for our task. Over the years, and throughout the highly contested discussions surrounding the EU AI Act, we have encountered a number of definitions. In the end, the definition of artificial intelligence sys-

1 Sheikh, H., Prins, C., Schrijvers, E. (2023): Artificial Intelligence: Definition and Background, in: Mission AI. Research for Policy. Springer, Cham. https://doi.org/10.1007/978-3-031-21448-6_2

2 Schank, Robert (1987): What Is AI, Anyway?, in: *AI Magazine* 8 (4) (© AAAI).

tems in the AI Act aligns with internationally recognised criteria and follows the OECD:

> a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

THE TECHNOLOGY EXPLAINED: artificial intelligence

Artificial Intelligence (AI) is the science and engineering of intelligent machines. It involves developing computer systems that can perform tasks requiring human intelligence, such as decision-making and problem-solving. AI has become a crucial part of our lives, revolutionising various industries, such as health care, finance and transportation. In a nutshell, Artificial Intelligence (AI) can be defined as the development of computer systems capable of performing tasks that require human intelligence. It involves decision-making, problem solving, object detection and many even more exciting things. AI has various components that enable it to function efficiently. These include learning, reasoning, problem-solving, perception and language understanding. Each component plays a crucial role in the overall functioning of AI systems.

It is important to know that a range of learning techniques are used. Let's dive into each of them:

1. Supervised learning: Here, the AI algorithm is trained using labelled data. The algorithm learns from this labelled data to make predictions or take actions based on new, unseen data. It's like having a teacher guiding the algorithm throughout the learning process.

2. Unsupervised learning: In this type of learning, the AI algorithm doesn't require any labelled data. Instead, it analyses the available data to identify patterns, relationships or clusters. It's as if the algorithm becomes a detective, trying to make sense of the data on its own.

3. Semi-supervised learning: This type of learning is a hybrid of supervised and unsupervised learning. It uses a small amount of labelled data along with a large amount of unlabelled data. It's like obtaining a few hints or clues to solve a puzzle, but still relying on your own intuition.

4. Reinforcement learning: In this type of learning, the AI algorithm learns by interacting with its environment and receiving feedback in the form of rewards or penalties. It's like playing a video game in which the algorithm learns by trial and error to achieve a specific goal.

These different types of learning techniques have played a crucial role in the development of AI systems and their ability to understand and interpret data. So, while AI may sound complex, it's fascinating to see how it mimics human learning and decision-making processes.

Although AI is hardly new, **the combination of immense data availability and stupendous computing power has led to its unprecedented growth**. Thanks to significant advances in data storage and transfer technologies, the amount of data being produced, recorded and processed has exploded. To illustrate, around four *billion* YouTube videos are watched each day. This abundance of online personal data, which includes digital footprints created by (or about) netizens, provides insights into their real-world behaviours, interactions and communication patterns.

Recent significant advances in user-friendly generative AI have led to the near-instantaneous production of text, images, audio and synthetic data. This has sparked a frenzy of new applications and developments, with certain products gaining widespread adoption at warp speed. For instance, ChatGPT amassed 100 million users within two months, a milestone that took Instagram two and a half years to reach. One of the reasons behind the popularity of generative AI tools is how convincing they are. It is hard to impress anybody with technology anymore, but many people were blown away by their initial interactions with these tools, which parrot human behaviour so well. But while they are already considered to be unstoppable, gen-

erative AI tools have also given rise to numerous ethical and legal issues. No policy area, whether it be democratic integrity, employment, education, market competition, art creation or science, will remain untouched.

Some people argue that AI is 'no big deal' and not fundamentally different from other technologies. They might stress that an AI system, like any other technological tool, is neither inherently good nor bad, likening it to a kitchen knife. But this is not true – **AI possesses unique characteristics that require sound governance, scrutiny and reflection**.

THE TECHNOLOGY EXPLAINED: bias, what makes AI different and not just another form of technology?

Part of the complexity of AI is that bias can creep in at any stage. Algorithms are often proprietary, complex and difficult to understand. Sometimes, they are effectively a black box, containing processes that may be inexplicable to a human researcher. This 'softwarisation' of bias means, for example, that existing inequalities end up coded in and perpetuated in obscure and intellectual property-protected machines.

In addition, algorithms can generate new categorisations based on seemingly innocuous characteristics, such as web browser preferences or apartment number, or more complicated categories that combine many data points. For example, an online store may find that most consumers using a certain web browser pay less attention to prices; the store can charge those consumers extra.

Artificial intelligence (AI) can unlock significant opportunities for individuals, organisations, businesses, the economy and society. AI can contribute to the development of life-saving advances in health care, enhance education and training, and facilitate the equitable distribution of opportunities. AI also powers many everyday products and services, and this is only likely to increase as the applica-

bility and usefulness of AI advances. In the past few months alone, our awareness of and interest in AI in our daily lives has increased significantly. The release of powerful new AI technologies to the general public – such as generative AI and large language models (LLMs) – has opened eyes and imaginations to AI's potential and versatility. We have seen that AI has the capability of powering the American economy by enabling innovation and productivity for a broader cross-section of the population. AI also has the potential to help address many of society's greatest challenges. It can assist with scientific discovery in the health and life sciences. It can help with climate science and sustainability. And it can help people survive or avoid natural disasters, with innovations such as wildfire and flood forecast alerts.

Like many new technologies, however, AI also presents challenges and risks to both individuals and society. For example, AI systems used to attract and retain talent in the workforce can expand opportunities, but could also amplify and perpetuate historical biases and discrimination at unprecedented speed and scale. Furthermore, AI could be misused in harmful ways, such as spreading disinformation or engaging in cybercrime. While AI systems could help to enhance access, such as accommodating individuals with disabilities or linguistic barriers, but it could also deliver incorrect diagnoses. AI could create economic opportunities or exacerbate the digital divide for individuals and communities. In the workforce, we are likely to see the growth of new occupations and the decline of others, as well as ongoing changes to many more. All such challenges magnify the need for appropriate AI oversight and safeguards. The balance we establish in addressing these two divergent AI realities – fully harnessing its benefits while also effectively addressing its challenges and risks – will significantly impact our future. If navigated appropriately, governments can ensure that AI creates greater opportunities, providing economic and societal benefits for a broader cross-section of the population. But if handled poorly, AI will further widen the

opportunity gap[3] and trustworthy AI for all may become an unrealised aspiration.

Part of what makes AI difficult to grasp is that it can creep in at any stage of the pipeline. Algorithms are often proprietary, complex and difficult to understand. Sometimes, they are effectively a black box, containing processes that may be inexplicable to a human researcher. This 'softwarisation' of, for example, bias means that existing inequalities can end up coded in and perpetuated in obscure and intellectual property-protected machines.

In addition, algorithms can generate new categorisations based on seemingly innocuous characteristics, such as web browser preferences or apartment number, or more complicated categories combining many data points. For example, an online store may find that most consumers using a certain web browser pay less attention to prices; the store can charge those consumers extra.

Because the source of these biases is not ultimately technological, they cannot be resolved using technology alone, but instead require a much greater degree of scrutiny and, to an extent, a positive social and political decision to overcome automated output that may simply be the product of historical data.[4] For example, if women have traditionally earned less than men, serving them adverts for higher paying jobs requires that employers make a conscious decision to try to overcome stereotypes and change existing patterns and limits on their talent pool.

3 The 'opportunity gap' describes how uncontrollable life factors such as race, language, economic and family situations can lead to lower rates of success in educational achievement, career prospects and other life aspirations (ref: the Close the Gap Foundation, https://www.closethegapfoundation.org/glossary/opportunity-gap)

4 Bartoletti, Ivana and Xenidis, Raphaële (2023): Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination. Council of Europe, available at https://rm.coe.int/prems-112923-gbr-2530-etude-sur-l-impact-de-ai-web-a5-1-2788-3289-7544/1680ac7936 (last accessed 11 January 2023).

FOCUS: What is bias in AI and do we have laws to curb it?

Bias in AI and algorithmic decision-making: 'Bias happens when seemingly innocuous programming takes on the prejudices either of its creators or the data it is fed'.[5] As a consequence, women (for example) may be denied credit, and speech recognition programs may misidentify words spoken by black people at much greater rates than for white people. Sofiya Noble's concept of 'algorithmic oppression' refers to this phenomenon, in which racist and sexist search results, targeted marketing and other forms of algorithmic data exploitation are not glitches in a purportedly unbiased information system but fundamental features of the operating system of the web.[6]

Examples of bias:

- In the Netherlands, the deployment of the SyRi system (System Risk Indication), used to detect social welfare fraud, was shown to cause discrimination on grounds of income and ethnic origin before being suspended by a court decision in 2020. In 2021, a welfare scandal forced the Dutch government to resign after more than 20,000 parents were flagged by an AI system as fraudsters in relation to childcare allowance and subjected to investigation by the Dutch tax authorities.[7] The AI system treated dual nationality as a high risk factor and this resulted in a disproportionate number of investigations and court proceedings being launched against families with an immigration background. Their child care

5 Garcia, Megan (2016): 'Racist in the Machine: The Disturbing Implications of Algorithmic Bias', in: *World Policy Journal* 33: 111–117.

6 Noble, Safiya (2018): *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press.

7 Benaissa, Nadia (2021): 'Het systeem doet precies wat het wordt opgedragen', in: *Bits of Freedom* (29 January), available at: https://www.bitsoffreedom.nl/2021/01/29/het-systeem-doet-precies-wat-het-wordt-opgedragen/.

benefits were suspended and some were required to repay benefits perceived. The case also shows how the lack of accountability and transparency around the use of these systems may deprive the subjects of AI decision-making of any explanation or an opportunity to appeal against decisions.

- In Spain, the VioGén software has been used to assess risks of gender-based violence and femicide by intimate partners. Despite an overall favourable assessment, criticisms point to several cases of false negatives, where low risk scores led to insufficient prevention efforts, with tragic consequences.[8]
- Reuters journalist Jeffrey Dastin reported in 2018 that Amazon had developed a program that relies on machine-learning to identify top candidates from CVs. The program systematically disadvantaged women's CVs because it reflected the gender gap in the workforce recruited over the previous ten years.[9]

The law: algorithmic discrimination may differ from 'traditional discrimination'. This is because algorithmic discrimination often happens by proxy, as the cases above demonstrate. For example, dual citizenship may act as a proxy for migration. In a nutshell, AI discrimination is not easy to identify and tackle, and there is no technical solution that may enable us to overcome it completely. For this reason, it is crucial that such systems be developed by diverse teams, and that strong controls are in place before and after release. In fact, debiasing can only be one element of a broader an-

8 Catanzaro, Michele (2020): 'In Spain, the VioGén algorithm attempts to forecast gender violence', in: *AlgorithmWatch* (27 April), available at: https://algorithmwatch.org/en/viogen-algorithm-gender-violence/ (last accessed 22 July 2022).

9 Dastin, J. (2018): 'Amazon scraps secret AI recruiting tool that showed bias against women', Reuters, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-airecruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G (last accessed 22 July 2022).

ti-discrimination strategy in relation to AI systems. Such a strategy should put human rights centre-stage and take account of the whole deployment cycle of algorithmic decision-making systems, ranging from formulation of the problem to be addressed, the context of implementation, actual performance and practical impact.

Large language models – the impact of generative AI

Large language models are complex neural networks trained on humungous amounts of data, extracted from essentially all written text accessible over the internet. They are typically characterised by a very large number of parameters – many billions or even trillions – whose values are learned by crunching this enormous set of 'training data'.[10] Through a process called unsupervised learning, large language models automatically learn meaningful representations (known as 'embeddings'), as well as semantic relationships among short segments of text. Then, given a prompt from a person, they use a probabilistic statistical approach to generate new text that sounds logical to the reader.

In its most elemental sense, what the neural network does is use a sequence of words to choose the next word to follow in the sequence, based on the likelihood of finding that particular word next in its training corpus. The neural network doesn't always just choose the most likely word, though. It can also select lower-ranked words, which gives it a degree of randomness – and therefore 'interestingness' – as opposed to generating the same thing every time. After adding the next word in the sequence, it just needs to rinse and repeat to build longer sequences. In this way, large language models can create very human-looking output, of various forms: stories, poems, tweets, whatever, all of which may appear indistinguishable from the works people produce.

10 IEEE Spectrum, available at: https://spectrum.ieee.org/ai-software.

Most will have heard of conversational AI, which refers to the deployment of automated AI-driven agents that engage individual human users in interactive dialogue. When text based, these systems are generally referred to as chatbots. When combined with natural voice generation and recognition, they are often referred to as virtual agents and can be used in call centres, as voice-based virtual assistants, and other spoken use-cases. When combined with simulated human faces that have an authentic appearance and can express interactive facial sentiments in authentic ways, they are referred to as virtual humans or virtual spokespeople (VSPs), especially when used to represent the specific interests of third parties through natural conversational interactions.

Some argue that current systems such as ChatGPT are not dangerous because they're text-based, but the industry is already shifting to real-time voice and photorealistic digital personas that look, move and express themselves like real people. This will enable the deployment of agenda-driven Virtual Spokespeople (VSPs) that are highly impactful and convincing. Nevertheless, some argue that the risks of manipulation are not new threats. After all, human salespeople already do the same thing, reading emotions and adjusting tactics. **Unfortunately, AI systems are likely to be far more perceptive than human representatives.** For example, AI systems can detect micro-expressions on human faces that are far too subtle for human observers. Similarly, AI systems can read faint changes in human complexion known as facial blood flow patterns and subtle changes in pupil dilation to assess emotions in real-time.

For all these reasons, some argue that conversational AI poses a significant threat to epistemic agency, namely the capacity to generate and control one's own beliefs.[11] When epistemic agency is compromised by new forms of media, a country's political establishment can undermine democratic institutions by deploying propaganda,

11 Rosenberg, Louis (2023): The Manipulation Problem: Conversational AI as a Threat to Epistemic Agency, 2023 CHI Workshop on Generative AI and HCI (GenAICHI 2023), Association for Computing Machinery, Hamburg Germany (April 28, 2023).

disinformation and misinformation that supports authoritarian objectives, interests or policies.[12] 'While current "influence campaigns" on social media are analogous to buckshot fired at broad groups, conversational agents could function more like "heat seeking missiles" that adapt their tactics in real time to maximise impact on individual users."[13] The existing rules and regulations that prevent abuses on traditional and social media may not protect us from the new personalised, interactive and strategic threats. Therefore law makers will have to enact forms of regulation to deal with this emerging danger. One possible approach could be to prevent platforms from using our emotional responses for their own benefit. Regulators should consider policies that ban platforms from tracking real-time emotions through vocal inflections, facial expressions or other biometric data to manipulate or persuade people.

The recent Digital Services Act (DSA), alongside the EU AI Act, do provide some guardrails for this. For example, the DSA makes it mandatory for large operators to provide transparency around the algorithms they use to serve content. The EU AI Act mentions 'subliminal techniques' that impair autonomous choice 'in ways that people are not consciously aware of, or even if aware, not able to control or resist' (Recital 16, EU Council version). Article 5 prohibits systems using subliminal techniques that modify people's decisions or actions in ways likely to cause significant harm. However, some argue that the definition of subliminal techniques remains unclear.[14] Many ethicists and legal scholars are concerned that the law might be interpreted too narrowly to offer meaningful protections while business stakeholders argue that the cost of complying with an overly broad interpretation might hamper innovation. A clear definition is needed that holds up to legal scrutiny and is defensible from a scientific and philosophical perspective, while not imposing excessive

12 Coeckelbergh, M. (2022): Democracy, epistemic agency, and AI: political epistemology in times of AI, in: *AI Ethics*, https://doi.org/10.1007/s43681-022-00239-4.

13 Ibid.

14 Vague concepts in the EU AI Act will not protect citizens from AI manipulation, https://oecd.ai/en/wonk/eu-ai-act-manipulation-definitions.

administrative and regulatory burdens.[15] This is a very complex area and one that clearly shows the urgency of robust guardrails around not only the collection of data but also its purposing. Machine learning that links personality and physical traits warrants critical review as it links to a much darker side of our past to the point that technology commentators have panned these facial-recognition technologies as 'literal phrenology',[16] comparing some applications to eugenics, phrenology's parent pseudoscience that aims to 'improve' the human race by encouraging those people deemed the fittest to reproduce, and discouraging childbearing in those deemed unfit.

The bottom line is that there is no good evidence that facial expressions reveal a person's feelings, and yet we are seeing a proliferation of big tech and start up products in this field. It therefore cries out for attention and watertight regulation.

The platformisation of our economy or the gig economy?

It is recognised that our world is going through a technological revolution that largely involves algorithms.

Platformisation can be defined as 'the penetration of infrastructures, economic processes and governmental frameworks of digital platforms in different economic sectors and spheres of life, as well

15 An excellent attempt at defining subliminal techniques can be found here. The author recommends the adoption of this definition by policymakers: Bermúdez, J.P. et al. (2023): 'What Is a Subliminal Technique? An Ethical Perspective on AI-Driven Influence,' 2023 IEEE International Symposium on Ethics in Engineering, Science, and Technology (ETHICS), West Lafayette, IN, USA, 2023, pp. 1-10, https://doi.org/10.1109/ETHICS57328.2023.10155039.

16 Crawford, Kate (2021): Artificial intelligence is misreading human emotion, in: *The Atlantic* (27 April), https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/.

as the reorganisation of cultural practices and imaginations around these platforms'.[17]

This has also affected the world of work. One impact is the 'platformisation of labour'. Platformisation refers to the proliferation of platforms that provide labour, connections as well services. Work is administered through these platforms.

There is no doubt that platform-based companies such as Uber, Airbnb and eBay have disrupted various sectors, including transportation, retail, travel and even personal relationships.

Online applications that connect users and transactions are aimed at instilling trust in customers. For example, the model underpinning Airbnb is very much the idea of an economy of trust and sharing, in which people feel that they can bypass traditional intermediaries and share directly.

However, 'not all these platforms are the same. If we look at the iconic gig economy platform Uber, what sets it apart from the others is the unique labour dynamic of controlling nearly four million drivers. Companies such as Uber perform as powerful organising intermediaries, connecting riders and their customers. In order to set fares and determine driver income, process payments, and provide feedback, the platform uses dynamic pricing models. Owing to Uber's algorithmic environment, this company has dominated the ride-sharing industry and disrupted transportation in more than 600 cities around the world."[18] The new development of algorithmic management, however, has led to a decrease in the quality of work and incentives to work beyond capacity. Much remains unknown about how platform workers engage with and are impacted by such management.

17 Poell, Thomas, Nieborg, David and Van Dijck, José (2019): Platformisation, in: *Policy Review*, 8, https://doi.org/10.14763/2019.4.1425.

18 McDaid, Emma, Andon, Paul and Free, Clinton (2023): Algorithmic management and the politics of demand: Control and resistance at Uber, in: *Accounting, Organizations and Society*, available at: https://doi.org/10.1016/j.aos.2023.101465.

The effects of these platforms on the way we live, purchase, work and enjoy our spare time are huge, and not just for individuals. Businesses too have had to adapt to this platformisation trend.

While the platform economy has brought some benefits, including convenience, and its boosters have therefore labelled it the 'creative economy' or the 'sharing economy', it has also introduced risks into the workforce, and is often referred to as the 'gig economy'.

These platforms frequently classify their service providers as independent contractors rather than employees, thereby depriving them of access to benefits normally available to regular employees. For example, independent contractors do not qualify for a minimum wage, overtime benefits, a pension, paid leave, sick leave, training opportunities or maternity leave and rights. These companies' 'flexibility' also means that service providers usually face job instability and uncertain earnings. Often in ridesharing, drivers work under pressure and are not compensated for any extra labour expended while not driving.

It is worth noting that all the above profoundly affects workers' interest representation. Contractors usually do not have the right to form a union, which weakens their bargaining power. For example, Uber requires drivers to sign arbitration contracts, preventing them from bringing class-action lawsuits.[19]

As mentioned earlier, platforms are very different. Airbnb, based on the notion of the 'shared economy', is very different from Wikipedia (shared knowledge building) or open-source software such as Linux or Apache. However, it is worth noting that platforms such as Uber or even Facebook do not really share. Rather, they 'monetise human efforts (....), Lyft and Airbnb are entrepreneurial initiatives

19 For a detailed overview of the externality of the platform economy, see the comprehensive and excellent study by Mosaad, Mohamed, Benoit, Sabine, and Jayawardhena, Chanaka (2023): The dark side of the sharing economy: a systematic literature review of externalities and their regulation, in: *Journal of Business Research*, 168, https://doi.org/10.1016/j.jbusres.2023.114186, (https://www.sciencedirect.com/science/article/pii/S0148296323005453).

that facilitate the conversion of consumption goods such as automobiles and apartments into goods that are monetized'.[20]

It is important to note that digital platforms are not merely digital. They are an amalgam of inextricably linked software, hardware, operations and networks. And if we take the definition of digital platforms as a 'place' where social and economic interactions are mediated online, often by apps, there is little doubt that digital platforms have been instrumental in entrenching the power of large technology companies. For example, many of the current internet platform firms use Amazon Web Services.

The platform phenomenon has grown mainly on the margins of the regulations that apply to the mainstream economy, resulting in distortions at national and local levels. Policymakers have spent the past few years grappling with the consequences of this and trying to regulate internet platforms. A key element of this has been a recognition of the rights of employees or of those whose incomes depend on these platforms. There is no doubt that while some workers, such as those employed by Microsoft, Google, LinkedIn and Facebook, retain traditional employment relationships, others do not. So the question is whether we are 'generating labor market flexibility, or a precariat that resembles a cyberised Downton Abbey replete with a small elite composed of the platform owners and a new and sizable underclass'.[21] In December 2023, in the Platform Work Directive, EU Member States and the European Parliament agreed industry rules that should allow workers, including Uber drivers and food delivery riders, to receive social security and other benefits.[22] Under the agreed proposals, companies that control workers' hours and what they wear at work, determine the amount of money workers can receive and restrict whether they can accept or turn down work will

20 *The Rise of the Platform Economy*, https://issues.org/rise-platform-economy-big-data-work/.

21 Ibid.

22 Council of the EU Press release, 13 December 2023, 'Rights for platform workers: Council and Parliament strike deal', https://www.consilium.europa.eu/en/press/press-releases/2023/12/13/rights-for-platform-workers-council-and-parliament-strike-deal/.

be subject to the presumption of an employment relationship and therefore will have to categorise such workers as employees and shoulder the corresponding costs.

The deal also includes the first EU rules on the use of so-called 'artificial intelligence' (AI) in the workplace, obliging companies to guarantee human oversight of their automated monitoring and decision-making systems. Furthermore, the Platform Work Directive aims to ensure the transparent use of algorithms in the workplace. As part of this, workers must be informed about the use of automated monitoring and decision-making systems. Additionally, the Directive prohibits digital labour platforms from processing personal data, for example, on a worker's emotional or psychological state, or related to private conversations, data used to predict actual or potential trade union activity, or to infer a worker's racial or ethnic origin, migration status, political opinions, religious beliefs, or health status, and finally biometric data, except for data used for authentication.

In this section, we have seen how the platformisation of work has led to the reshaping of work and employment. It is important to point out, however, that platforms are not only technical systems but also market systems. Their emergence is the outcome not only of data mining and mobile technologies but also of interlocking domains, including business, commerce, technology and logistics. While some progress has been made, the term 'platform' has clearly also been used by business journalists and internet companies to draw in end-users to and simultaneously to obfuscate their business models and technological infrastructures.[23]

23 Couldry, N. (2015): The myth of 'us': digital networks, political change and the production of collectivity, in: *Information, Communication & Society*, 18(6), 608–626. https://doi.org/10.1080/1369118X.2014.979216.

AI and labour: algorithmic management of work – or worker surveillance?

Digitalisation has entered the workplace in many other ways. Especially during the Covid-19 pandemic and thanks to remote working, work surveillance has increased dramatically. This has meant the proliferation of tools tracking employees' attention, connection times and wider attendance. This has raised concerns amongst policymakers, as well as trade unions.

In a nutshell, algorithmic management of work is a diverse set of technological tools and techniques that structure the conditions of work and remotely manage workforces. It is important to recognise the relevant nuances, however, some of which are related to what was described in the previous section in relation to the platform or gig economy. In this section, we will look at how AI and automated decision-making has come to affect the workforce and started to replace human decision-making, including hiring and firing.

While often considered to be more reliable, less biased and more precise than the choices made by humans, algorithmic management of work is fraught with issues. Human resources is an area in which the role of digitalisation and automation is increasing. This includes tools that purport to read emotions during interviews, and others that scan CVs, evaluate performance and grade job applicants. The list is very long and there are many vendors offering these products mainly to larger companies with a promise of increased efficiency, bias reduction and more objectivity in the selection and rating of candidates. While the promise is certain there, the reality has not yet matched it. This is because, as previously argued, AI-driven technological tools of this kind are in fact a bundle of data, people and parameters and are therefore prone to 'softwarising' existing inequalities into decision-making. For this reason, as we will discuss later, EU legislators have defined such products as 'high risk AI', thus subjecting them to at least some control.

Another area worth mentioning is wellness and benefits, Over the past decade, employee health and wellness benefits have become in-

creasingly popular. Supporters of such benefits argue that they benefit both workers, making them healthier and more productive, and employers, who ultimately save money. However, data is collected and transmitted in mysterious ways, leaving workers struggling to navigate a complex system of benefits. Employers' involvement in worker wellness raises concerns about privacy, discrimination, penalties for non-participation, surveillance and even criminalisation. A recent US report[24] defines the plethora of work-based wellbeing initiative as a sort of 'wellness capitalism'. This is because of the 'benefits maze' of unproven, data-collecting tech products that could have serious unforeseen consequences. These issues highlight the potential risks and benefits of data-driven technologies in the workplace.

Public services or the administrative state?

The role of the state has changed too, with two main factors that, combined, are creating both new opportunities and risks, and require novel approaches.

The first is the digitalisation of public services and the second is the novel interdependence between the public and private sectors, with the big technology companies playing an increasing role. These two elements cannot be seen as independent as the intensification of the latter has led to an increase digitalisation of the administrative state.

First it is important to recognise how effective and efficient government and the transformation of the public sector are highly dependent on data. The provision of programmes and services is based mainly on data verification, determining individuals' suitability or eligibility for benefits, as well as monitoring and maintaining environmental resources. Additionally, policy research relies heavily on data, and evidence-based decision-making is vital for sound govern-

24 Nopper, Tamara K. and Zelickson, Eve (2023): Wellness Capitalism: Employee Health, the Benefits Maze, and Worker Control, in: *Data & Society* (21 June), https://datasociety.net/library/wellness-capitalism-employee-health-the-benefits-maze-and-worker-control/.

ance. Therefore, the value of data as a strategic asset is recognised by governments and organisations worldwide. Using various technologies and techniques, governments can obtain real-time data, which is crucial for effective decision-making, especially during crises such as the Covid-19 pandemic.

In times of emergency, governments can use data harvesting to assess the impact of the situation on the affected population. This becomes particularly important for providing timely responses and aid, especially in disaster relief efforts. The availability of rapid and accurate information feedback loops is crucial for good decision-making in urgent situations. A recent study shows how new Big Data sources – such as satellite and aerial imagery, drone videos, sensor web networks, the internet of things, spatial data, crowdsourcing, real-time social media, and mobile GPS and telecoms – can be employed during disaster relief operations. Furthermore, data harvesting can also help people to better understand their own lives and the environment in which they live. Harvesting a wide range of data and making it accessible and relevant can help to keep people informed about issues that affect their quality of life, and perhaps lead them to make different decisions and choices.

Recognising the importance of data for local and national governments also entails being fully aware of the potential risks.

First, we have seen how tech-driven provision of services, predictions and allocation of resources can be appealing to public administrations that have been deprived of the financial resources they need to deal with increased demand. Algorithms can of course deliver savings but they are fraught with challenges, including inherent biases and lack of transparency when they are embedded in existing AI solutions. This means that public sector agencies may end up being lured into procuring systems that deliver the savings they need without understanding what they are purchasing.

As already mentioned, the harms that these systems may give rise to are severe. In the Netherlands, the deployment of the SyRi system (System Risk Indication), used to detect social welfare fraud, was shown to cause discrimination on grounds of income and ethnic origin. Its use was terminated by a court decision in 2020. In 2021,

a welfare scandal forced the Dutch government to resign after more than 20,000 parents had been flagged by an AI system as fraudsters in relation to child care allowance and subjected to investigation by the Dutch tax authorities. The AI system treated dual nationality as a high risk factor and this resulted in a disproportionate number of investigations and court proceedings being launched against families with an immigration background, whose child care benefits were suspended and some were required to repay benefits.

This was not the only case. In Spain the VioGén software has been used to assess risks of gender-based violence and femicide by intimate partners. Despite a favourable assessment overall, criticisms point to several cases of false negatives where low risk scores led to insufficient prevention, with tragic consequences.[25]

Bias is not the only issue, although its consequences may indeed be disastrous, especially for the most vulnerable.

This is where the relationship between governments and big tech companies comes in. As we have seen, governments are increasingly relying on large companies for data harvesting. This trend became apparent during the Covid-19 pandemic. In the midst of the pandemic, Google Meet became a delivery mechanism for schools. AmazonFresh made it possible to shop for groceries without braving the supermarket. And there is more, as governments around the world have resorted to tracking technology and other data-driven tools in order to monitor citizens. These tools have all been provided by big tech, which has seized the opportunity to forge even closer links with governments.

Local governments have developed interesting examples of data harnessing for the common good by forging initiatives to resist the predatory practices of big tech, as well as to build new forms of data citizenship. An interesting example of urban data ownership and

25 Catanzaro, Michele (2020): In Spain, the VioGén algorithm attempts to forecast gender violence, in: AlgorithmWatch (27 April), https://algorithmwatch.org/en/viogen-algorithm-gender-violence/ (last accessed 22 July 2022).

control is the New Data Deal[26] launched in Barcelona, which showcases a city government trying to regain access and control over urban data for the benefit of its citizens.

Monitoring and surveillance

To some extent, we can say that surveillance is part and parcel of the modern state and constitutes a key feature of bureaucratic administration for purposes such as tracking compliance. Citizens are indeed surveilled, and the digitalisation of services – coupled with the pervasiveness of tracking tools and partnerships with big tech, whose business model is often underpinned by data extraction – is accelerating this process at high speed.

Clearly, surveillance has negative connotations. Indeed, the word itself prompts a visceral reaction among some, especially because it recalls the depredations of certain past regimes. This is especially strong when people perceive tracking as veering into areas of control and influence. Arguably, however, digital tools allow a continuum between surveillance as 'benevolent' tracking and surveillance as control. This is because of these tools' capabilities. For example, facial recognition technology not only assists with tackling crime (especially without adequate social policies), it also changes the way citizens behave in public spaces. It remains to be seen what the long-term effects will be of *knowing* one is being watched at all times, or of becoming accustomed to it. While in the past we might leave a trail made up of smells or objects, we now leave a recorded trail in stores, often 'tagged' with our names. This represents a profound shift in how we live our lives, and one whose consequences are still not being studied in sufficient depth.

26 Fernandez-Monge, F., Barns, S., Kattel, R., and Bria, F. (2023): Reclaiming data for improved city governance: Barcelona's New Data Deal, in: *Urban Studies*, https://doi.org/10.1177/00420980231204835.

Blockchain and decentralisation

Blockchain technology is a decentralised structure with the potential to transform traditional trust-based systems. With the massive growth of digital transactions, blockchain builds on the need for autonomous and trustless systems.

Decentralisation aims to replace centralised intermediaries with distributed networks, thereby removing the need for a trusted central authority. Traditional trust-based systems are highly susceptible to fraud, corruption and censorship because of their centralised nature. Blockchain technology provides a more secure and efficient way of ensuring trust while maintaining autonomy.

Simply put, Blockchain is a secure and tamperproof way to share valuable data. It is a digital database composed of encrypted blocks of data that are chained together. It acts as a decentralised digital ledger that records all transactions made on a network of computers. Each computer on this network creates a copy of the ledger, and any additions or changes made to the ledger must be verified by the network, which makes it nearly impossible to manipulate the data stored on it.

THE TECHNOLOGY EXPLAINED: Blockchain and decentralisation

Understanding blockchain: Blockchain is a decentralised, immutable ledger of transactions shared across a network of computers. Its key features are transparency, security and decentralisation. Applications that utilise blockchain include cryptocurrencies, supply chain management, and voting systems. Blockchain enables users to transact peer-to-peer without intermediaries, thus increasing efficiency and trust.

Decentralisation refers to the transfer of control and decision-making from a centralised entity (individual, organisation or group) to a distributed network. Decentralisation is important because it promotes transparency and security, and reduces the

risk of a single point of failure. Types of decentralisation include political, administrative and financial.

Blockchain enables decentralisation by creating a secure and transparent digital ledger that can be accessed by anyone. However, decentralisation also poses challenges such as data privacy and regulatory compliance. Its impact on society is still evolving. There are numerous applications of blockchain. In health care, examples include decentralised storage of patient data, clinical trial research, pharma supply chain management, staff credential verification, and remote patient monitoring. In finance, examples include smart contracts, digital currencies, cross-border payments, and regulatory compliance. Voting, intellectual property, energy, insurance and education are other areas in which blockchain is deployed.

Blockchain's most significant advantage is the level of security it provides. Over time, the blocks in the chain become more secure because the network adds more blocks, making it challenging to alter previous ones. This makes it the perfect solution for storing sensitive data.

In a traditional transaction system, one central authority verifies and validates transactions. In the case of the blockchain system, each node has a copy of the complete blockchain, which is continually updated. When a transaction is initiated, it is validated by several nodes before it is added to the ledger.

The role of decentralisation in blockchain is vital because it ensures that no single entity controls the system. That means that the data stored on the blockchain is not vulnerable to a single point of failure. As a result, it becomes nearly impossible for hackers to compromise the blockchain network.

There are three types of blockchain: public, private and hybrid. Public blockchains, such as Bitcoin, are open to all and are fully decentralised. Private blockchains are used within organisations and are accessible only to authorised users. Hybrid blockchains are a combination of both and are used in enterprise-level projects.

There are a number of advantages to using blockchain technology. It enables rapid, low-cost and secure transactions; eliminates the need for a central authority to oversee financial transactions; and has the potential to boost financial inclusion in areas in which traditional banking services are scarce. However, risks around governance and especially around privacy have also emerged, especially because of blockchain's immutability (the ability of a blockchain ledger to remain a permanent, indelible and unalterable history of transactions).

The metaverse

The metaverse is a collection of technologies that can merge our physical and virtual lives. During the Covid-19 pandemic, lockdown measures showed us that it's possible to migrate online for learning, work, communication and entertainment, without any stigma. The metaverse, however, is still an intangible concept that draws on various technologies, such as online platforms, blockchains, and virtual and augmented reality. It is expected to offer virtual offices and immersive health care, enabling people in remote areas to access them easily. Gaming and online shopping are some of the areas in which immersive experiences are already prevalent.

In conclusion, the metaverse is a mainly intangible experience composed of a persistent network of virtual worlds, data and supporting systems. Physical devices and AI systems are still the gateways to access and create these experiences, however, meaning that Big Tech companies and other private actors have significant soft and hard power in defining this new world. Moreover, because a decent online connection is the (perhaps obvious) indispensable condition for accessing the metaverse, the current digital divide is a key limitation. **According to the UNDP, in fact, nearly 37 per cent of people worldwide still have no access to the internet, especially in developing countries, rural areas and, if belonging to certain social groups, women.**

And finally ... 5G and connectivity

Connectivity has come a long way since the advent of the internet. From the first mobile phones to wireless broadband, internet connectivity has evolved rapidly over the years. In recent times, the introduction of 5G technology has created an exciting buzz in the tech world. 5G, or fifth generation, is the latest innovation in wireless technology promising higher speeds, lower latency and greater capacity.

For those unsure about what connectivity is, it is the ability to connect devices and people to the internet. This has enabled an explosion in technological advances and has practically created a digital world that transcends geographical boundaries. The evolution of connectivity technology has changed the way we communicate, shop, work and learn on a global scale.

5G technology takes internet connectivity to the next level, with speeds of up to 20 gigabytes per second, as well as low latency and more capacity. Its potential impact on our society is vast and includes revolutionary changes from advances in health care and telemedicine to transportation systems and smart cities.

The arrival of 5G technology brings with it a host of exciting possibilities and implications in a wide variety of industries. One major area in which 5G is already starting to have an impact is health care and telemedicine. With 5G's lightning-fast speeds, medical professionals can share large data files and images in real time, leading to more accurate diagnoses and better patient outcomes. Additionally, remote patient monitoring and consultation are made feasible by 5G networks' low latency and high capacity.

5G technology is also set to revolutionise transportation systems. Autonomous vehicles will require real-time data transfer to navigate roadways safely, and 5G networks are capable of providing such information in a split second with minimal delay. This could lead to a surge in eco-friendly, autonomous ride-sharing services, potentially reducing the number of cars on the road and the amount of harmful emissions being produced.

In smart cities, 5G presents opportunities to develop efficient and effective public infrastructure systems, from energy grids to transportation. This infrastructure could be made more intelligent and responsive with sensors and connected devices communicating through 5G networks. This presents opportunities for cities not only to become more eco-friendly but also to become more responsive to their citizens' needs, resulting in improved quality of life.

The imminent introduction of 5G technology across the EU is expected to bring new opportunities for citizens and businesses, through faster internet browsing, streaming and downloading, as well as through better connectivity. However, 5G, along with 3G and 4G, with which it will operate in parallel for several years, also pose threats.

One of the primary concerns is cybersecurity. As more devices are connected to the internet and higher volumes of data are transferred, cyber attacks and data breaches are a very real risk.

Secondly, there is a debate on 5G's impact on human health. This is because xG networks operate within several different frequency bands, and there are plans to use much higher radio frequencies at later stages of the 5G technology evolution. Traditionally, the proposed new bands have been used for radar and microwave links and very few have been studied to assess their impact on human health. A recent study by STOA[27] evaluated current knowledge of both carcinogenic and reproductive/developmental hazards of radio frequencies as utilised by 5G.

Another key point is the investment required for 5G infrastructure. The transition to 5G networks demands significant investment in both hardware and software upgrades. This investment is a significant hurdle for many countries, particularly developing nations, and could create (or exacerbate) a digital divide between those who can afford it and those who cannot.

Crucially, 5G will also increase privacy risks. Not only will we be able to connect and process more data (more devices, more data),

27 Health impact of 5G, https://op.europa.eu/en/publication-detail/-/publication/0d329c11-570b-11ec-91ac-01aa75ed71a1/language-en.

but granularity will also increase and more accurate geolocation data will be generated on networks. Satellite positioning systems, such as GPS or Galileo, which drive numerous location-based consumer services (for example, for navigation or fitness tracking) will provide a far higher degree of accuracy. Finally, it is worth noting that 5G is likely to be deployed in wealthier cities before it is deployed in poorer ones or rural areas. Therefore, insights from 5G network data or data from applications viable only in an area of 5G deployment may be inherently biased in relation to wealthier metropolitan populations. This is important as uncritical data use may lead to harmful policy decisions.

PART II:
The European Union between the competition, sovereignty and the Brussels effect

Introduction

In the past ten years, there has been an upsurge in legislation and other political measures around data, the digital ecosystem and the infrastructure supporting it.

In this chapter, we will analyse the main tenets of the EU's stance on the digital realm and take a close look at the numerous initiatives launched in recent years and decades.

Importantly, the European Commission declared 2020–2030 to be Europe's 'digital decade' and set 'technological sovereignty' and 'digital sovereignty'[28] as key strategic goals. That is the clear context and framework for what follows.

It is important to remind ourselves at the outset what the term 'sovereignty' means here. In a 2020 strategy paper, the European Parliament defined digital sovereignty as 'Europe's ability to act independently in the digital world'. It warned that '[s]trong concerns have been raised over the economic and social influence of non-EU technology companies' and that EU citizens' control over their personal data was in danger. Furthermore, 'the growth of EU high-technology companies and the ability of national and EU rule-makers to enforce their laws' are constrained (when EU digital sovereignty is in jeopardy).[29]

28 European Commission, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_4630.

29 European Parliamentary Research Service (2020, July): Digital sovereignty for Europe, https://www.europarl.europa.eu/RegData/etudes/

The term 'technological sovereignty' is often used to point to a general lack of investment in specific sectors, for example in the chip industry. This is particularly complex (and political) terrain, especially bearing in mind the China–Taiwan dynamic and the evolving US position on it. That is why the EU adopted a European Chips Act[30] that is intended to address semiconductor chip shortages by mobilising more than 43 billion euros (€) of public and private investments. It also envisages other measures to anticipate and respond to future supply chain disruptions.

A lot of what Europe has done in the digital space can indeed be seen through the prism of sovereignty. We often hear how the General Data Protection Regulation (GDPR) has had global impact, sparking debate around privacy and data protection in other jurisdictions. The same wave effect characterises the AI Act, the world's first explicitly AI-focused legislation (although AI is already regulated in many places and in many ways). We will discuss this further on in this primer.

It is crucial to understand that technical and digital sovereignty is the thread binding together the EU's policy position on digital matters. Before moving on to analyse developments in more detail, it is also important to register the part played by several major events and factors in sharpening the appetite for sovereignty.

First, the Covid-19 pandemic shone a harsh light on European dependence on large US tech companies not only to provide contact tracing apps and other pandemic goods and services, but also to maintain 'business as usual' in the rest of the economy. It also vividly highlighted the West's dependence on the Asian market and its manufacturers, which were severely affected by the pandemic.

All this demonstrated that being able to hold one's own in global supply chains is perhaps the most real and 'gritty' element of sovereignty. This gave rise to a rethinking of priorities and the emergence of novel approaches.

BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf (accessed on 7 September 2022).

30 European Commission (2023), European Chips Act, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en.

Russia's invasion of Ukraine and its wider geopolitical implications have compounded the problems. As a result, the European Union perhaps has a keener appreciation of how its sovereignty is linked to the United States.

The creation of the EU–US Trade and Technology Council (TTC) is perhaps the most visible expression of efforts to foster an alliance on democratic technology. Although a European initiative, the TTC held its inaugural meeting in Pittsburgh, Pennsylvania, on 29 September 2021. Europe's overarching goal has been pursued under the TTC banner of 'values-based digital transformation'.

The European approach, proposing and participating in the TTC, bears the hallmarks of the EU's digital foreign policy strategy, based on the so-called 'Brussels effect'. For instance, the EU's pioneering act on AI regulation, designed to prevent the exploitation of this technology for illicit and unethical purposes, has faced criticisms that it might 'inhibit innovation'. Nevertheless, a working group was set up to cooperate on AI policy. Recently, this working group released an AI glossary. This is a pragmatic, but also very symbolic way of trying at least to speak the same language, beginning with the main definitions around AI.

Here is the TCC's purpose in its own words:

> The European Union and the United States are partners strongly committed to driving digital transformation and cooperating on new technologies based on their shared democratic values, including respect for human rights.
>
> The EU-US Trade and Technology Council serves as a forum for the United States and the European Union to coordinate approaches to key global trade, economic, and technology issues and to deepen transatlantic trade and economic relations based on these shared values. It was established during the EU-US Summit on 15 June 2021 in Brussels.[31]

31 European Commission, EU-US Trade and Technology Council, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en.

Along with the deepening of this partnership – which we will examine more closely– we have seen a slew of initiatives pushing the sovereignty agenda. These include moves and instincts that we could define as 'data protectionism' or even 'data nationalism', namely attempts to leverage the use of data for a particular nation's growth and benefit. Data protectionism has shown its face in various places, from controversies around the cross-border sharing of personal data, to more subtle requirements around data residence and localisation. We will examine this shortly.

The point we need to underline is that while governments across the world seem to be caught up in a whirl of data protection, data protectionism and sovereignty, the reality of large corporations exists in parallel, transcending borders like the internet itself.

Data is power

In the previous chapter we saw how the digital ecosystem has evolved, from phones to apps, to generative AI and the quest for decentralisation. How the internet's penetration into the lives of European citizens, the widespread use of digital devices and the Internet of Things have together led to the emergence of big data and updated analytical technologies.

All of this is transforming trade and impacting global politics. Even more than other elements of the global economy, data is intertwined with power. Accumulation of, and access to, data has become a geopolitical matter. The power of data has fundamentally reshaped the power structures in our societies, starting with the rise of Big Tech companies.

The expansion of the Big Tech companies exemplifies a data-centric model of production. The accumulation of data, its analysis and mastery has led to the centralisation of a vast amount of power in the hands of these large corporations (not least those with the resources to own and run vast, energy-hungry server farms), and a shift of power from the state to non-state actors.

Recognising the scale of that power shift is fundamentally important.

Big Tech companies have focused on the collection of data. **They have constructed a digital ecosystem to strengthen and expand their ability to rule the ecosystem itself in a way that transcends both virtual and actual borders.** And, as described in the preceding chapter, when Big Tech assumes certain public service functions, it erodes power that was long felt to be more appropriate for democratic states.

The combination of all these factors explains how the European Union's position on digital policy can be broadly broken down into the following strands.

(i) Initiatives aimed at containing the power of large digital platforms and at promoting more efficient competition. These initiatives include the Digital Markets Act, the Digital Services Act, as well as several antitrust investigations boosted by a number of sanctions and judgments.

(ii) A number of actions aimed directly at promoting digital and tech sovereignty. These include the the Data Governance Act and the upcoming Data Act, as well as the emerging GAIA-X project, which could perhaps be scaled up into a fully fledged European Cloud Federation.

(iii) The institutionalisation of the European Union as a global regulator. This strand involves the GDPR, as well as the EU AI Act.

(iv) Closely intertwined with the above, the last strand comprises several initiatives aimed at bringing together innovation and citizens' fundamental rights. This is perhaps the most complex area, and one we will focus on further.

Reining in big tech

The Digital Markets Act[32] (DMA) is aimed at regulating the so-called gatekeeper platforms, in other words the large commercial providers of core platform services, such as search engines, online intermediation and social networking. The European Commission´s standpoint is that these gatekeepers 'are entrenched in digital markets, leading to significant dependencies of many business users on these gatekeepers, which leads, in certain cases, to unfair behaviour vis-à-vis these business users'. Studies commissioned during the impact assessment for the Digital Markets Act arrived at the same conclusion: in the language of competition policy, there is a core 'theory of harm'[33] in the Digital Markets Act.

The Digital Markets Act defines and prohibits unfair business practices on the part of the major online platforms that are deemed problematic. The criteria for gatekeeper status imply that a firm must have a major impact on the EU market.

Specifically, a company must meet the following conditions to be considered a gatekeeper: it must offer a key platform service that acts as a critical gateway for business customers to reach end-users, as a result of which it 'has (or is about to have) an entrenched and durable position in the market'; annual turnover of no less than €7.5 billion within the EU for the previous three financial years or an average market valuation of at least €75 billion during the past financial year; it has to provide the same core platform service in at least three Member States. The following are the different types of online entities that provide intermediary services: third-party electronic commerce markets such as Amazon and eBay, online search engines, social networking services, video-sharing service platforms, virtual assistants, cloud computing services such as Google Cloud, and online advertising services, including advertising networks, advertising

32 European Commission, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

33 In other words, it explains why that conduct harms competition and should be prohibited.

exchanges, and any other intermediary advertising services, such as Facebook Ads and Google Ads, provided by a company that offers one of the basic platform services listed above.

Gatekeepers have a number of obligations, especially concerning the protection of personal data. Article 5, paragraph 2 of the Digital Markets Act (DMA) stipulates that gatekeepers cannot use the personal data of end-users who depend on third-party services that use the gatekeeper's basic platform services for online advertising purposes.

They are also barred from combining personal data collected through the basic platform service with data collected through other platform services or any other services provided by the gatekeeper or third-party services. Furthermore, gatekeepers are prohibited from cross-utilising personal data from the basic platform service to other services provided separately by the gatekeeper. Unless specific consent is provided, gatekeepers cannot register end-users to access other gatekeeper services to combine their data.

The Digital Markets Act establishes a new advisory committee for digital markets, which is responsible for assisting the European Commission in enforcing the Act's provisions. Non-compliance can result in significant fines or corrective measures.

If intentional or negligent non-compliance by gatekeepers is discovered, the Commission can levy fines up to 10 per cent of the gatekeeper's global annual revenue or 20 per cent for repeated violations, in addition to daily payments of up to 5 per cent of total global daily revenue. Systematic infractions may result in further corrective measures, such as structural remedies or a ban on acquiring any company providing digital or data collection services affected by non-compliance.

In short, the goal of the Digital Markets Act is to bring about competitive balance among companies operating in the digital sector, which has long been under the complete control of big players, as a result of which it lacks the necessary equity and competition. The Digital Markets Act's provisions aim to ensure such equity and contestability.

The Digital Markets Act needs to be seen alongside the **Digital Services Act**[34] (DSA).

To ensure the smooth and efficient functioning of the EU's internal market for digital services, the Digital Services Act amends existing regulations based on the principle that illegitimate activities offline should also be considered illegal online.

The Act applies to multiple classes of digital services, including, but not limited to, online markets, social networks, content sharing platforms, online travel and accommodation platforms, app stores, intermediary services (such as domain registers and internet providers), cloud and web hosting services, and collaborative economy platforms, all identified together in the Act as 'information society services', or intermediaries that offer services telematically or electronically, frequently for a fee.

The Directive aims to create a secure and trustworthy online setting that safeguards consumers' rights and, at the same time, promotes innovation and competitiveness. By accelerating the procedure for eliminating illegal content and improving public supervision of online platforms – primarily the most popular ones that impact over 10 per cent of the European population – the goals of the Digital Services Act include, among other things, protecting consumer rights, reducing the spread of illicit content, information manipulation and online disinformation, and providing consumers and businesses with access to a greater selection of digital services at lower cost.

The Digital Services Act (DSA) has preserved the E-Commerce Directive's guidelines, but it has introduced new rules regarding transparency, informational commitments and accountability.

The relevant obligations are proportional to the service type and number of users. For this reason, intermediary service platforms are grouped into four categories: intermediary services, online platforms (for example, social media), hosting (for example, the cloud), and

34 European Commission, Digital Services Act, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

very large platforms. Each category includes specific commitments that must be met within four months after assignment.

The primary obligations, which are common to all types, explicitly indicate the service conditions and their requirements, offering clear information on content moderation and the use of algorithms for content recommendation systems, which users can still reject. There must also be transparency in relation to recommendation systems and online advertising that is aimed at users, avoiding targeted advertising directed at children or based on sensitive user data. Deceptive practices that manipulate user choices, such as dark patterns, are prohibited and tech companies must cooperate with national authorities when requested.

THE TECHNOLOGY EXPLAINED: dark patterns

Dark patterns are a range of behavioural and design techniques used to influence consumer choice online, in ways that exploit cognitive biases and can be detrimental to the consumer. For example, the 'Unsubscribe' button may be tiny, low-contrast and buried in paragraphs of text at the bottom of an email. Another example is using obscure language, or legalese, to trick users into giving a particular response. Not all dark patterns are designed maliciously, however, and some UX designers might not even be aware that they've built a system that is misleading users.

The new obligations include reporting crimes, creating a complaint and recourse mechanism, adopting measures against abusive reports and replies, and checking third-party providers' credentials according to the 'know your business customer' (KYBC) principle, including random checks.

Large online platforms and search engines with a user base of 45 million per month or more[35] pose greater risks, so the Digital Ser-

35 The DSA classifies platforms or search engines that have more than 45 million users per month in the EU as very large online platforms

vices Act obliges them to comply with stricter requirements, such as risk management, emergency response, and prevention of system abuse. Moreover, such platforms are required to share their key data and algorithms with the authorities and authorised researchers to enable them to comprehend the evolution of online risks, collaborate in emergency responses, respect specific codes of conduct, and prevent systemic risks, such as the diffusion of illegal content or content that violates fundamental rights. Another obligation is to encourage independent audits, for example, to examine the correctness of financial data and applied procedures, enabling users to block recommendations that are based on profiling. Mere conduit activities (basic transport, caching, and hosting) providers are exempted from the new obligations. These activities do not establish accountability for the information stored at the service recipient's request, provided that the provider is unaware of any illegal activities or content.

Once made aware, a provider must act swiftly to remove the illegal content or restrict access to it. Sanctions for DSA violations may cost the violator up to 6 per cent of total annual turnover, and damages or losses caused by platform infringement can be compensated. The DSA can sanction platforms for submitting incorrect, incomplete or misleading information, failing to correct submitted information, and failing inspections. In such cases, Article 42 of the Digital Services Act stipulates that sanctions must be less than 1 per cent of annual income.

(VLOPs) or very large online search engines (VLOSEs). The Commission has begun to designate them as VLOPs or VLOSEs based on user numbers provided by the platform or search engines, which, regardless of size, they were required to publish by 17 February 2023. Platforms and search engines will need to update these figures at least every six months.

The link between data, personal data and competition

As we have seen in the previous chapter, data accumulation and the amassing of large quantities of personal information underpin the business models of big tech companies. The latter have gained prominence and power and indeed quasi utility status, albeit without the controls and strict governance to which utility companies (such as water or gas providers) are subject.

All over the world, countries taking measures to try to rein in this power. The quest to limit these companies' ever-expanding power is similar from China to the United States, although the focus may differ. In China the supremacy of state control is the main issue, while in the United States it is rooted in a more traditional antitrust approach.

EU legislators have frequently warned that existing Big Tech players – many of which already own vast swathes of the online economy – are gobbling up new parts of the digital landscape, often via killer acquisitions[36] of nascent competitors that have yet to break into the mainstream. Such concerns lie behind the ways in which the Digital Markets Act significantly restricts how certain so-called gatekeeping digital giants, or tech firms with an outsized footprint, can expand their businesses. Many smaller tech companies across Europe are pinning their hopes on this Act, the EU's first overhaul of the rules governing internet competition for 20 years, to give them a chance to compete against the giants fairly. The hope is that this antitrust legislation will transform how these giant companies do business, disabling their core strategy of integration that has allowed them to tie in users, dominate markets, and capture billions of euros in revenues.

A particularly interesting feature of current efforts to tackle anticompetitive behaviour is that they seem to be moving beyond demands for behavioural changes. For example, it can be argued that

36 In a 'killer acquisition' a company acquires control of an innovative company to eliminate them as a possible source of future competition.

the abovementioned legislative initiatives are only operating in the margins. They **prescribe a series of behavioural changes** but fail to tackle the root cause of the problem, which is these firms' combination of size and data.

In a recent formal antitrust complaint against Google[37] and its ad business, however, the regulator mentioned in its preliminary opinion that Google has abused its dominant position in the digital advertising market. It says that forcing Google to sell off parts of its business may be the only remedy if the company is found guilty as charged.

This would be a significant move, targeting the main source of the search giant's revenue, and a rare example of the EU recommending divestiture at this stage in an investigation. The Commission has already fined Google over three prior antitrust cases, but previously it has only imposed changes to its business practices.

Recently, pressure has been growing for Brussels to investigate specific data-related elements of these transactions.

For instance, Amazon's proposed $1.7 billion acquisition of iRobot, the creator of automated vacuum cleaner Roomba, was closely scrutinised[38] to determine whether it would give Amazon an unfair market edge. The antitrust investigators have shifted their attention to a relatively new area of interest that raises concerns about privacy and data protection. Specifically, the inquiry aims to examine whether iRobot would collect and use sensitive information, such as details about households and behaviour that could further entrench Amazon's competitive advantage.

This type of data-related scrutiny is not entirely unfamiliar to regulatory entities as similar deals have attracted attention over the years.

37 Antitrust: Commission sends Statement of Objections to Google over abusive practices in online advertising technology, European Commission, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3207.

38 Amazon's iRobot Roomba acquisition under formal EU investigation, in: *The Verge*, https://www.theverge.com/2023/7/6/23628636/eu-regulators-amazon-irobot-roomba-acquisition-investigation.

In 2020, Brussels launched a large-scale investigation after Google acquired Fitbit.[39] There was uncertainty about whether Google would use the data generated from the many Fitbit users to target ads and threaten competitors. Although there were concerns that this and similar acquisitions would allow major tech giants to purchase potential competitors and strengthen their dominance, the regulators assented to Google's purchase of Fitbit after concluding that this was not the case.

Interestingly, a recent judgment from Europe's highest court provided some clarity concerning the intersection between privacy and competition law. There is no doubt, in fact, that although the two regimes are different (privacy is about human rights and human dignity, while competition is concerned with market functioning), there are areas of convergence that cannot be ignored.

In July 2023, Meta lost its fight against a German data curb order that strikes at the heart of its business model as Europe's top court backed the German antitrust watchdog's power to also investigate privacy breaches. The ruling[40] from the Luxembourg-based Court of Justice of the European Union (CJEU) potentially bestows more leeway on antitrust authorities in Big Tech probes. The interesting element of this case is that it was centred on the German cartel authority's request that the social media giant stop collecting users' data without their consent, calling the practice an abuse of market power. At issue was whether the German antitrust agency had overstepped its authority by using its antitrust power to address data protection concerns, which are the remit of national data protection authorities. The CJEU, in this landmark case, created new jurisprudence at the intersection of antitrust and data protection law by deciding that an abuse of dominant position in digital markets can be found by an antitrust authority on the basis of a breach of the GDPR.

39 European Commission, Press Release: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484.

40 InfoCuria case – law, https://curia.europa.eu/juris/documents.jsf?num=C-252/21.

Regulation of the online ecosystem and the functioning of its market is a rapidly evolving area, and it remains to be seen whether tinkering in the margins through behavioural changes will suffice – or whether these large corporations have become too big to be reined in.

Sovereignty: a complex concept with an EU flavour

'There is no longer any political sovereignty without technological sovereignty', French economy minister Bruno Le Maire said last year, calling for 'a European technological awakening'. And technological sovereignty has indeed dominated public discourse in Europe over the past few years.

Some significant tech companies are based in Europe, including Nokia, Ericsson, Spotify, Skype and Booking. Most of these firms have not been able to take the lead in their respective categories, however.

During the last technology revolution, Europe was not able to develop tech giants like Google, Facebook and eBay, which are all based in the United States. Subsequently, the United States has been able to create up to 50 per cent of the world's so-called 'unicorns',[41] followed by China, India, and the United Kingdom. Among EU countries, Germany and France have the largest shares in the top 10, albeit with only 2.6 per cent and 2 per cent shares, respectively.[42]

Although Europe is home to some of the world's most exceptional universities and researchers, it lags behind the United States and China in research and development (R&D) spending. The European Commission's top 10 spenders on corporate research include only one European company, Volkswagen AG.

41 A tech 'unicorn' is a privately held technology-based startup company that has a valuation of over $1 billion.

42 Wanat, Zosia (2023): Will Europe's dream of tech sovereignty ever become reality?, in: *Sifted*, https://sifted.eu/articles/europes-tech-sovereignty-ever-become-reality.

The consensus is that Europe has made notable contributions to the tech industry, but it has not attained a pivotal position in most sectors. An often invoked solution is to increase investment in research and development (R&D) to compete effectively with other countries, such as the United States and China, which are the top R&D spenders.

The startup ecosystem Is similar. The statistics on investment in startups show a similar imbalance between Europe and the United States. According to Dealroom statistics, European startups secured funding of $95.7 billion, whereas US startups raised $241.5 billion in 2022. Funding rounds appear to be bigger in the United States, with a median series A round of $13.7 million compared with Europe's $10 million in 2022.

In light of the above, several European countries have established new public funds to support innovations in the fields of deeptech and climate tech. One example is Germany's fund,[43] which is worth €1 billion and seeks to support growth-stage companies involved in deeptech and climate tech. Similarly, France's deeptech startups have access to a €500 million fund. Poland's climate tech fund of funds worth €55 million also enables investments in deeptech ventures. Furthermore, a new Czech fund has been set up to support artificial intelligence (AI) spinouts. These public funds are important because they help to encourage the growth of important technologies that can benefit societies while also stimulating economic development.

The EU's strategy for sovereignty in data space aims to create a single market for data that will allow it to flow freely *within* the EU and across sectors for the benefit of businesses, researchers and public administrations. The signs are that this is making some of the big tech companies rather nervous, and we can expect to see some bruising encounters in the years ahead between emboldened states

43 Partington, Miriam (2023): Germany launches €1bn fund for climate and deeptech scaleups, in: *Sifted*, https://sifted.eu/articles/germany-1bn-deeptech-climate-fund-news.

and tech titans defending the territory they conquered with remarkable speed and have no desire to relinquish.

The Data Governance Act[44] and the Data Act[45], the Free Flow of Non-Personal Data Regulation and the Open Data Directive should be viewed in this context.

The Data Governance Act and the Data Act are part of the European strategy for data, presented by the European Commission in February 2020. This strategy aims to develop a single market for data by supporting responsible access, sharing and re-use, while respecting EU values and in particular the protection of personal data. As already mentioned, this should be seen in the broader context of the European Commission's action plan to ensure Europe's digital sovereignty by 2030. It is complementary to the European strategy on artificial intelligence.

The Data Governance Act was adopted in May 2022 and was set to come into force in September 2023. It aims to promote the sharing of personal and non-personal data by setting up intermediation structures. This regulation includes guidance and technical and legal assistance to facilitate the re-use of certain categories of protected public sector data (confidential business information, intellectual property, personal data); mandatory certification for providers of data intermediation services; and optional certification for organisations practising data altruism.

In the wake of the Data Governance Act, the upcoming Data Act is the second main proposal issued recently as part of the European strategy for data and complements the existing data framework: the General Data Protection Regulation (GDPR), the Free Flow of Non-Personal Data Regulation and the Open Data Directive. A number of other forthcoming regulations will also impact the current data rules, such as the Digital Markets Act or the Digital Services Act, which were discussed above in relation to competition and user transparency.

44 EU Data Governance Act: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act.

45 EU Data Act, EU Commission: https://www.eu-data-act.com/.

Legislative initiatives in this area include the EU Data Act, which aims to provide a regulatory framework to govern and make easier the sharing, use and re-use of internet or product-generated data. It also aims to make it easier to switch between cloud providers.

The Act applies primarily to manufacturers, suppliers and users of IoT devices and related services. It also applies to 'data holders' that make data available to data recipients in the EU, public sector bodies in certain situations and data processing services providers, and to cloud service providers. Data holders (that is, manufacturers/service providers with initial control of IoT data) must give users (owners or renters of an IoT product) ready access to the data generated about them. Cloud providers will be subject to a range of obligations to help users switch to another provider, including a right for customers to terminate at two months' notice (the exact period is currently being debated). They must also implement technical measures to safeguard against non-EU government access to IoT data that they hold that may conflict with EU laws. There are also provisions related to minimum interoperability standards for operators of European data spaces and minimum standards for smart contracts used for data sharing.

The Free flow of non-personal data in the European Union Regulation[46] ('FFDR') entered into force on 28 May 2019. Together with the GDPR, the FFDR establishes a legal framework for the free flow of all data in the EU and aims to create a basis for developing the data economy and enhancing the competitiveness of the data industry in the EU. Where the GDPR ensures the free flow of personal data, the FFDR aims to ensure the free flow of other forms of data.

The FFDR applies to the processing of electronic data other than personal data in the EU, where (1) the data originally does not relate to an identified or identifiable natural person or (2) data which was initially personal data but was later anonymised.

The FFDR also regulates the status of mixed datasets, composed of both personal and non-personal data, which represent the ma-

46 Free flow of non-personal data, https://digital-strategy.ec.europa.eu/en/policies/non-personal-data.

jority of datasets used in the data economy today. In a dataset composed of both personal and non-personal data, the FFDR applies to the non-personal data part of the dataset and the GDPR to the personal part.

Where personal and non-personal data in a dataset are inextricably linked, however, the data protection rights and obligations stemming from the GDPR apply in full to the whole mixed dataset, also when personal data represents only a small part of the dataset.

One of the purposes of the FFDR is to avoid vendor lock-in practices. As a result of such practices users cannot switch between service providers because their data is 'locked' in the provider's system, for instance because of a specific data format or contractual arrangements and cannot be transferred outside the vendor's IT system. Porting data without hindrance is important because it allows users to choose freely between providers of data processing services and thus ensures effective market competition.

To this end, the FFDR prohibits, as a rule, EU Member States from imposing requirements on where data should be localised. Exceptions to this rule may be possible only on grounds of public security in compliance with the proportionality principle; a cooperation mechanism must be established to ensure that competent authorities may continue to be able to exercise any rights they have to access data being processed in another EU Member State; and incentives are provided for industries, with the support of the Commission, to develop self-regulatory codes of conduct on switching service providers and porting data.

It is worth bearing in mind that the Data Governance Act, as well as the Data Act, will intersect with the FFDR (discussed above). It remains to be seen how the interplay between all the EU data-related legal initiatives plays out when they are all in force and are being enforced by regulators in the coming years.

Institutionalisation of EU regulatory power

The theme of sovereignty is strongly intertwined with the EU's attempt to establish itself as a global rule setter in the digital realm.

A number of initiatives can be viewed as heading in this direction. The first is the General Data Protection Regulation (GDPR), a comprehensive data protection law that governs the collection, use and storage of individuals' personal data within the European Union (EU). It came into force on 25 May 2018, replacing the EU's previous data protection directive.

The GDPR aims to give EU citizens more control over their personal data, as well as to establish more harmonisation and consistency in the approach to data protection across EU Member States. It can be argued that, first and foremost, it concerns rule setting at EU level to promote the cross-sharing of data within the Union, thus facilitating commerce and enabling growth.

In relation to the GDPR, organisations must adhere to (and demonstrate how they may achieve compliance, in accordance with the accountability principle, which is arguably the most important) stricter rules on how they collect, process and store personal data. The GDPR also empowers individuals with more control over their data by giving them the right to access, modify and have their data erased. Privacy by Design is a principle that requires organisations to ensure data protection and lies at the core of their data processing activities. Data Protection Officers must be appointed by organisations that process large amounts of personal data. Data Breach Notifications must be reported to the relevant authorities within 72 hours of becoming aware of the breach.

The GDPR has had a significant impact on data protection throughout the EU. It has brought in stricter rules and regulations concerning the collection, storage and use of personal data. This has increased the responsibility of data controllers and processors to safeguard the information they hold. Non-compliance can result in severe penalties, which has made the issue even more pressing. This includes fines of up to €20 million or 4 per cent of global turnover.

As a result, the GDPR has transformed data protection and privacy laws across the world, becoming a benchmark for countries looking to strengthen their regulations.

The European AI Act

The European Commission proposed the European AI Act in 2021. At the time of writing, a political agreement has been reached between the European Parliament and the Member States through the (rather obscure) trilogue process. The outcome of this process was by no means a foregone conclusion as some countries (Germany, Italy and France) called for less stringent requirements for the sake of European competitiveness. Eventually, a political agreement was found in December 2023, making the Act the first AI-specific legislation in the Western world.

The Act stems from a product legislation approach (so it is not context-specific but horizontal). This applies controls to AI based on the risks they pose. High-risk AI includes products deployed in the following areas: biometric identification and categorisation of natural persons; management and operation of critical infrastructure (road traffic, water, has, heating and electricity supply); education and vocational training; employment, worker management and access to self-employment; access to and enjoyment of essential private services and public services and benefits; law enforcement; migration, asylum and border control management; administration of justice; and democratic processes.

AI systems that present an 'unacceptable risk' – for example, 'practices that have a significant potential to manipulate persons through subliminal techniques beyond their consciousness or exploit vulnerabilities of specific vulnerable groups such as children or persons with disabilities in order to materially distort their behaviour in a manner that is likely to cause them or another person psychological or physical harm' – are prohibited. AI systems that present a limited risk are subjected to specific transparency obligations and those with low or minimal risk to codes of conduct.

The EU AI Act also covers general purpose AI. This kind of AI is what we have grown accustomed to since ChatGPT hit the market. A

general-purpose AI is artificial intelligence that can be used for many different purposes. For example, foundation models are large systems capable of performing a wide range of distinctive tasks, such as generating video, text and images, conversing in lateral language, computing, or generating computer code. Although at the time of writing we do not have all the details, the political agreement reached seems to introduce a special regime for so-called general-purpose AI (GPAI) systems, and the GPAI models they are based on. This special regime strongly emphasises transparency. In particular, general purpose AI systems that can cause systemic risks have several obligations, including risk management, robustness and cybersecurity, including red teaming, and energy consumption monitoring and disclosure. An agreement was also reached on copyright, with regard to which GPAI providers must adopt policies that adhere to EU copyright laws.

Unacceptable risk: Prohibited AI practices Title II (Article 5) of the proposed AI act explicitly bans harmful AI practices that are considered to be a clear threat to people's safety, livelihoods and rights, because of the ‚unacceptable risk' they create.

For the sake of clarity, it would be prohibited to place on the market, put into service or use in the EU:

- biometric categorisation systems that use sensitive characteristics (such as political, religious or philosophical beliefs, sexual orientation, race);
- untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases;
- emotion recognition in the workplace and educational institutions;
- social scoring based on social behaviour or personal characteristics;
- AI systems that manipulate people's behaviour to circumvent their free will; and
- AI used to exploit people's vulnerabilities (age, disability, social or economic situation).

The draft text distinguishes between two categories of high-risk AI systems.

High risk: Regulated high-risk AI systems Title III (Article 6) of the proposed AI act regulates 'high-risk' AI systems that create adverse impact on people's safety or their fundamental rights. The draft text distinguishes between two categories of high-risk AI systems.

- Systems used as a safety component of a product or falling under EU health and safety harmonisation legislation (such as toys, aviation, cars, medical devices, lifts).
- Systems deployed in specific areas identified in Annex III, which the Commission could update as necessary through delegated acts (Article 7):
  - biometric identification and categorisation of natural persons;
  - management and operation of critical infrastructure;
  - education and vocational training;
  - employment, worker management and access to self-employment;
  - access to and enjoyment of essential private services and public services and benefits;
  - law enforcement;
  - migration, asylum and border control management;
  - administration of justice and democratic processes.

All these high-risk AI systems would be subject to a set of new rules, including:

- **A required ex-ante conformity assessment:** Providers of high-risk AI systems would be required to register their systems in an EU-wide database managed by the Commission before putting them on the market or into service. Any AI products and services governed by existing product safety legislation will fall under existing third-party conformity frame-

works (for example, for medical devices). Providers of AI systems not currently governed by EU legislation would have to conduct their own conformity assessment (self-assessment) to show that they comply with the new requirements and are entitled to use CE marking. Only high-risk AI systems used for biometric identification would require a conformity assessment by a 'notified body'.

- **Other requirements:** Such high-risk AI systems would have to comply with a range of requirements particularly on risk management, testing, technical robustness, data training and data governance, transparency, human oversight, and cybersecurity (Articles 8 to 15). They would also need a specific assessment of such systems' impact on fundamental rights. In this regard, providers, importers, distributors and users of high-risk AI systems would have to meet a range of obligations. Providers from outside the EU will require an authorised representative in the EU to, among other things, ensure the conformity assessment, establish a post-market monitoring system and take corrective action as needed. AI systems that conform to the new harmonised EU standards, currently under development, would benefit from a presumption of conformity with the draft AI act requirements.

A point on facial recognition

Special consideration must be given to facial recognition, as AI powers the use of biometric technologies, including facial recognition technologies (FRTs), which are used by private or public actors for verification, identification and categorisation purposes. In addition to the existing legislation (for example, data protection and non-discrimination), the AI Act also covers facial recognition technologies, although this is a highly contested area: several countries wanted exceptions for national security. According to information from

the political agreement,[47] the use of real-time Remote Biometric Identification (RBI) facial systems in publicly accessible spaces for the purpose of law enforcement would be prohibited, unless Member States choose to authorise them for important public security reasons, such as searching for specific suspects in the investigation of a serious crime or, for example, the imminent threat of a terrorist attack, and only if the appropriate judicial or administrative authorisations are granted.[48]

Finally:

Limited risk: transparency obligations

AI systems presenting 'limited risk', such as systems that interact with humans (for example, chatbots), emotion recognition systems, biometric categorisation systems, and AI systems that generate or manipulate images, audio or video content (for example, deepfakes), would be subject to a limited set of transparency obligations.

Low or minimal risk: no obligations

All other AI systems presenting only low or minimal risk could be developed and used in the EU without conforming to any additional legal obligations. However, the proposed AI Act envisages the creation of codes of conduct to encourage providers of non-high-risk AI systems to voluntarily apply the mandatory requirements for high-risk AI systems.

THE TECHNOLOGY EXPLAINED: facial recognition

Facial recognition technology (FRT) is a type of biometric recognition technology that uses artificial intelligence (AI) to identify individuals through their facial features. The impact of such technology may be heightened by the context in which it is deployed.

47 European Parliament, Press Release, 09-12-2023, 'Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI', https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai

48 For an overview, see Madiega, T. and Mildebrath, H. (2021): Regulating facial recognition in the EU, EPRS (September).

For example, it is increasingly being adopted by police agencies, immigration authorities, universities and retailers.

What risks are connected with facial recognition technology? In public services, the use of such technology can lead to the exclusion of certain users from access to public services. For example, a photo booth at the State Office of Transportation in Hamburg, Germany, failed to recognise an applicant's face for the purpose of taking a biometric picture, which she needed for her administrative application. Even though the public office denied that the failure was due to the facial recognition software, one employee indicated that such failures often take place depending on applicants' skin colour.[49]

FRT technologies, often coupled with emotional recognition capabilities, have exhibited severe risks of discrimination.[50] In addition, FRT may introduce profound changes into society. A feeling that one is being watched in public spaces and in real time inevitably changes how one experiences shared environments and how one behaves with others.

The debate on the European AI Act has been heated over the past few years, especially towards the end of the process as the Spanish Presidency pushed for an agreement before the end of 2023. The EU Act reflects the pull of two different poles: on one hand, governments hoping to score points with their electorates and thus demanding exemptions for national security purposes and to try to boost the competitiveness of their own companies; on the other hand, MEPs, often in partnership with civil society groups, who (generally) have

49 Wulf, J. (2022): Automated decision-making systems and discrimination: understanding causes, recognizing cases, supporting those affected, in: *AlgorithmWatch*, p. 8.

50 Buolamwini, J. and Gebru, T. (2018): Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research; Devlin, Hannah (2020): AI systems claiming to ‚read' emotions pose discrimination risks, in: *The Guardian* (16 February), https://www.theguardian.com/technology/2020/feb/16/ai-systems-claiming-to-read-emotions-pose-discrimination-risks

sought to uphold European values. One key example of this tension is the area of emotional recognition. MEPs wanted to ban this altogether as unacceptable to Europeans, especially because of the lack of scientific proof underlying it. Governments, by contrast, pushed for it as a vital element in their fight against crime. The upshot is that emotional analysis has been banned in education and at work, but is still permitted in migration control.

It is still too early for a verdict on the Act, of course, and much remains to be debated in meetings on the technical details. However, it is important to recognise that compromise lies at the heart of these processes. The fact that the AI Act includes (at the time of writing) the requirement of a Fundamental Rights Impact Assessment for high-risk AI speaks to MEPs' vocal advocacy and determination alongside civil society organisations to ensure that AI works for people, not against them.

The EU AI Act is the first AI law in the world. It will of course need finetuning and review, and the courts will play their part in interpreting it. But we ought to celebrate the fact that the EU is a pioneer in AI legislation.

The EU as a global regulator? The Brussels effect

In 2012, Anu Bradford observed that the European Union has a 'strong and growing ability to promulgate regulations that become entrenched in the legal frameworks of developed and developing markets alike, leading to a notable "Europeanization" of many important aspects of global commerce',[51] She calls this an 'unprecedented and deeply underestimated' regulatory power that the EU is able to exercise via its 'legal institutions and standards'. Bradford coined the term the 'Brussels effect' to describe this European ability 'to exercise power beyond its borders as well as its mechanism of setting standards and then requiring compliance with these standards to gain or have continued access to the European single market, a significant marketplace and economic player in global affairs'.[52]

In her 2012 article, Bradford cites the examples of antitrust laws, privacy regulation, regulation of chemicals for health protection, environmental protection, and food safety and focuses on legal and ideological differences between the EU and the United States, as well as the European ability to influence US standards effectively.

This is also evident in the European ambition to set the rules of the digital realm. It is also important in this connection to understand how broad the Brussels effect is. Take the case of *Schrems II*.[53] Data

51 Bradford, A. (2012): The Brussels effect, in: *Northwestern University Law Review*, 107 (1), Columbia Law and Economics Working Paper No. 533, Available at SSRN: https://ssrn.com/abstract=2770634

52 Bendiek, A. and Stuerzer, I. (2023): The Brussels Effect, European Regulatory Power and Political Capital: Evidence for Mutually Reinforcing Internal and External Dimensions of the Brussels Effect from the European Digital Policy Debate, DISO 2, 5 (2023), https://doi.org/10.1007/s44206-022-00031-1

53 *Schrems II* is the most commonly used abbreviation for *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (C-311/18), a case brought by Max Schrems, an Austrian lawyer, privacy advocate, and founder of NOYB, an organisation dedicated to bringing legal cases concerning data protection under the GDPR to EU courts. As its name suggests, however, the *Schrems II* case was the second high-profile case

protection regulations have been highly contested in recent times, especially since the European Court of Justice (ECJ) voided the 'privacy shield' (the transatlantic agreement regulating the exchange of users' private data between European company subsidiaries and their American holding companies for commercial purposes) in *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems* in July 2020. To date, the EU has failed to implement a new framework, with dire consequences for the companies concerned. For instance, the Austrian data protection authority banned the use of the data analysis tool Google Analytics, which was a significant setback for Google but also for Austrian companies that used the tool. We have witnessed similar cases across the EU and consequently businesses have struggled with the risks involved in international data flows and their impact on their everyday activities.

The influence of the Brussels effect even on US legislative debates illustrates how it may help shape legislation far beyond the EU. The *Schrems II* case has fostered further debates on federal law, as well as on possible reform of the US surveillance system. The key point about *Schrems II* is indeed the long-term harm done by US surveillance practices, especially to people outside the United States. Discussions around privacy are currently gaining momentum, and have even been embraced very publicly (if selectively) by large companies themselves, perhaps motivated by a desire to prevent a proliferation of laws that add to what is often resented as the 'burden' of compliance.

In data privacy as well as machine learning/artificial intelligence, the EU's efforts to function as global regulator have their roots in its attempt to win the competition game by setting the rules of the game, especially as no large company in this sector is based in the EU.

Schrems has brought in relation to international data transfers between the EU and the United States. Ref: Data Guidance, https://www.dataguidance.com/resource/definitive-guide-schrems-ii.

5G and microchips: sovereignty in action

Notwithstanding the EU's ambition to compete on a global scale, the Brussels effect has its drawbacks.

The most evident of these is that as of 2019 none of the top fifteen digital companies were based in Europe. Currently, Europe lacks its own leading computer or mobile operating system, messaging service, or browser, indicating a heavy reliance on foreign software.

This reflects the fact that technology is now infiltrating all sectors through shared technologies such as artificial intelligence and cloud computing. Europe's overall corporate performance is lacklustre. A sample of over 2,000 American and European companies, each with revenues exceeding $1 billion, were analysed using McKinsey's Corporate Performance and Analytics Tool (CPAT) to try to understand the disparities in corporate achievement. Findings revealed that from 2014 to 2019 larger European companies were 20 per cent less profitable, based on return on invested capital (ROIC). Furthermore, their revenue growth was 40 per cent slower, their capital expenditure was 8 per cent lower relative to the stock of invested capital, and their R&D expenditure was 40 per cent less than other companies in the sample.

This can be traced back to the fact that Europe did not keep up with the United States during the initial technology wave focused on the internet and software. This leaves Europe in a compromised position when it comes to shared technological advancements across various sectors.

There is better news for Europe in the case of 5G, in relation to which we are seeing some interesting developments. The EU has long invested in security standards, cybersecurity and cyber resilience as a way both of leveraging its internal market and rewarding (or excluding) companies. The case of Huawei is one of the best known of such tussles. Huawei was the first company in the world to build and run infrastructure based on 5G. But when it expressed an interest in investing in connectivity in Europe, at affordable cost, the EU pushed back. The bloc was worried about the expansion on its territory of a company controlled by the Chinese government. It was

feared that allowing Huawei to build critical infrastructure could and would be exploited to gain access to EU confidential information.

The case of Huawei is interesting because it shows what role that the EU can play and the strength of its hand. By going as far as threatening to fine Huawei, the EU demonstrated a degree of unity and credibility that surprised many. The Brussels effect is rooted in the power of having 27 Member States legislating through democratic procedures, a power that is likely to be taken more seriously going forward.

But the EU is not primarily concerned with keeping others out. The fact that the leading US technology company in 5G, Intel, decided to invest in Europe can be seen as confirmation of that. The EU's unity on 5G generated credibility and thus political capital. This in turn has attracted US investment.

Semiconductors (or chips) are a key component of digital manufacturing that the EU wants to make for itself. The EU Chips Act demonstrates the same assertiveness as its approach to 5G. Its aim is to reverse the trend of outsourcing semiconductor production overseas, as a keystone of its wider programme to regain industrial capacity and technological sovereignty and to reduce its vulnerabilities. Four months after its introduction, there is some evidence that the EU Chips Act is already spurring investment. Early and promising signs include Intel's commitment to build a $19 billion semiconductor plant in Germany as part of a stated investment in Europe of $90 billion. STMicroelectronics and GlobalFoundries signed up with the French government for a $6 billion chip factory in France. Other semiconductor manufacturers from the United States and Taiwan, besides European companies, are drawing up investment plans for Europe.

This is certainly encouraging although the United States and the EU are still dependent on international producers. The United States and the EU together account for 21 per cent of the world's semiconductor manufacturing capacity, but consume 43 per cent of the global output of digital devices, which highlights a potentially dangerous dependency on Chinese manufacturers. There are of course producers of semiconductors in Europe, too. For example,

Dutch company ASML is the largest supplier for the semiconductor industry and the sole supplier in the world of extreme ultraviolet lithography (EUV) photolithography machines that are required to manufacture the most advanced chips.[54] On the other hand, when it comes to producing the actual chips, Germany's Infineon has been consistently ranked the tenth or eleventh largest chip company in the world for the past five years, while just three giant companies account for roughly half of all global semiconductor sales: Samsung (South Korea), Intel (US) and TSMC (Taiwan).

The complexity of the discussions around the EU Chips Act shows how hotly contested technological sovereignty is, and how tightly bound up with power dynamics between nations and blocs. We will discuss later how sovereignty can be leveraged, not in terms of autarchy (rather the opposite) but in terms of navigating and standing tall in a global and complex supply chain.

54 Some general information on ASML: https://en.wikipedia.org/wiki/ASML_Holding. And an article from the *Michigan Journal of Economics*: https://sites.lsa.umich.edu/mje/2023/04/05/asml-the-little-known-source-of-the-worlds-technological-progress/.

PART III:
A path forward: opportunities and challenges for Europe

It is not easy to define a path forward for the EU in the digital realm. It needs a multi-layered approach and a suite of initiatives that bundle together different interests and often conflicting priorities. For example, the need to boost the single market may be at odds with recent protectionist tendencies that we are seeing even in the EU itself.

We shall analyse this later. For now, we need to focus on understanding the most useful power the EU has at its disposal, which is undoubtedly its potential geopolitical influence.

Digital and technological sovereignty: breaking dependence and aiming for constructive leadership

In the previous chapter, we saw how the EU is taking action to mitigate some of the risks of its dependence on a very complex global supply-chain and digital ecosystem.

This dependence comes at a cost and highlights some contradictions within the EU's policy approach. For example, in France the new Health Data Hub – a platform designed to centralise and provide access to data from patients, health practitioners and hospitals – is operated by Microsoft because of the lack of a homegrown French alternative that meets the government's requirements. More recently, Oracle signed a deal with the European Commission to provide Oracle Cloud Infrastructure (OCI) and its platform services across EU administrations.

With *Schrems II* and the ECJ's annulment of the Privacy Shield, however, the French data regulation body (CNIL) has stopped any French data from being shared with (or accessed by) the United States. Similar debates took place during the Covid-19 pandemic in relation to contact-tracing apps and the dominance of large American companies in delivering them.

This has affected consumers and voters, whose perspective matters enormously. As their attention is drawn to the crying lack of homegrown applications, systems and platforms to cope with national crises they see huge sums of public money flowing to large tech providers based far away. Justified or not, their disappointment has to be handled and may be felt at the ballot box. When Meta released Thread, it made it clear that it would not release it in Europe because of Europe's complex privacy laws and wary approach to AI. Lobbying has certainly played a part. It is no secret that large corporations have lobbied vigorously against the EU AI Act. For example, OpenAI's Sam Altman personally embarked on a grand tour of Europe and its leaders.

It may be an effective strategy to threaten to pull out of the EU, or to cut EU consumers out of enjoying shiny new products at launch. It may capture consumers' attention and focus it on what they imagine they might be missing out on (the products) rather than on the considerable benefits they would enjoy by having superior privacy protection. In the case of OpenAI, the company introduced a number of protections, but not before the Italian regulator decided to halt the processing of European data by ChatGPT. Altman's company nevertheless did come up with some useful guarantees, including deletion of chats and some safeguards around data retention, but 'by reaction' rather than 'by design'.

There is no doubt, however, that breaking the cycle of tech dependency is a tall order – and it may even turn out to be unachievable

But large platforms are not the only issue. Europe also relies on non-EU actors in other areas, for example cloud computing. And cloud companies are playing a larger role in the broader tech stack,[55] moving from 'infrastructure as a service' (IaaS) to 'platform as a service' (PaaS) and to much more, including the whole data space, thus impinging even more on the digital B2B ecosystem.

The cloud is not the only issue. We have seen how 'the digital' is about more than the web; it is also about chips and cables. The EU is lagging behind in the development of its own submarine cables and satellite-based communications. This is critical. A number of American platforms have made inroads into these strategic fields. For example, a coalition led by Facebook, including Orange, will build a 37,000 km cable to link 23 African countries with the Middle East and Europe. Most American digital companies are also investing heavily in launching satellites that will play a key role in telecommunications.[56]

Space exploration has profound economic and geopolitical implications, too. It facilitates the provision of services in remote areas that previously were cut off from online connectivity. However, the advent of phone packages through satellite systems provided by a range of players could endanger Europe's autonomy. It could strengthen these players' dominance in various branches of the communications sector, highlighting the importance of infrastructure diversity and freedom of choice for both businesses and consumers. It is vital to implement the policy measures needed to ensure that the pursuit of space technology does not compromise Europe's sov-

55 A tech stack – also known as a solutions stack – is a combination of technologies used by companies to build and run a website or application.

56 European Digital Sovereignty, Institut Montaigne, https://www.institutmontaigne.org/en/expressions/digital-compass-europes-digital-sovereignty

ereignty in the long term.[57] In early 2023, Europe announced that – inspired by Elon Musk's Starlink[58] – it will launch its own space satellites aimed at expanding its citizens' connectivity and digital communications. These satellites were named the IRIS² Satellite Constellation. The European Union already had satellite constellations, such as Galileo, which is used for navigation systems like the American GPS and Copernicus for observing planet Earth.

The investment in IRIS² reinforces the need to seek digital sovereignty in a context in which economic and security concerns are growing, along with cyber threats, which makes them increasingly dependent on fast and resilient connections.

The EU expects that satellites will be at their full operating capacity as early as 2027. This provides little time for the project to become one of the continent's strategic points of security, resilience and protection.

But what is tech sovereignty?

Tech sovereignty is perhaps the buzzword of our times. Since the outbreak of the Covid-19 crisis, politicians across the spectrum have been pushing to reduce Europe's dependence on US or Chinese technologies. From vaccine development to artificial intelligence, billions of euros are now being mobilised across the European Union. And the rhetoric never ceases.

Many agendas come under the aegis of tech sovereignty. The term is interchangeable with several similar terms that have also gained

57 Ibid.

58 After Russia's invasion of Ukraine and under pressure from Ukrainian minister Mykhailo Federov for Elon Musk to provide Starlink services in the territory under attack, SpaceX sent the necessary equipment so that the satellites could be used.
Starlink has proved to be valuable, especially in a conflict environment, because the more satellites there are in orbit, the more complex it is for a possible enemy to cut off their communications. It would be necessary to destroy thousands of mini satellites for that to happen and the budget for an operation at that level would be prohibitive.

great political traction over the past year. One might mention 'strategic autonomy', 'regulatory sovereignty' and, increasingly, 'digital sovereignty'. The scaled-up rhetoric speaks to **a growing recognition that Europe must compete better in key areas, focus urgently on security of imports of vital goods, and limit the reach of US and Chinese technology**.

Does tech sovereignty make sense? Yes, it does. A progressive argument around tech sovereignty must be rooted in three elements, however:

(i) The ability to stand tall in the global supply chain, and recognition that we must not, and cannot, confuse sovereignty with nationalism or protectionism.
(ii) The capacity to generate demand within the EU, and to leverage it to foster the EU's technology ecosystem.
(iii) The ability to create a culture of investment, growth and risk to harness the value of Europe's business and technology.
(iv) The ambition to see Europe's sovereignty through the lens of sustainability, which in turn can generate demand and boost Europe's standing in the world.

Generating demand

- Generating demand is essential. Nurturing internal demand for services entails generating data and, as a consequence, data-driven services. This applies to companies that need to digitise rapidly, as well as to public service provision, which needs to go digital. Businesses and the public sector need to move up a gear with their ICT stack and deploy AI and generative AI to boost productivity in order to foster demand for digital services and to create value in Europe.
- Similarly, the European Commission's very concrete targets will enhance the role of public actors in creating demand for digital services. These include the ambition to achieve 100 per cent online provision of key public services for European citizens and businesses, to give 100 per cent of European citizens

access to electronic medical records, and to enable 80 per cent of European citizens to use digital ID.

- Generating data – especially industrial data – will be essential, so investing in data-sharing mechanisms will be very important to harness the EU single market through tools such as the Data Act and the Data Governance Act.
- There must be research and investment in the intersection between AI and open data. AI tools can provide value for open data, especially as Europe will soon have common standards on generative AI. This will be a great advantage. For example, genAI can be used in cities. Larger cities will be able to create their own LLMs, generate comprehensive city planning scenarios based on urban development data, or create personalised learning plans for students based on education data. Governments could also develop AI 'public assistants' that can explain complex legislation, provide real-time updates on policy changes, or guide citizens through bureaucratic procedures. Such AI assistants could democratise access to public information, reduce administrative burdens, and enhance civic engagement. Census ChatGPT could generate real-time, data-driven insights about demographic trends, socio-economic disparities, housing statistics, and more.
- Innovation in digital markets can be promoted by enhancing **interoperability**, which requires that the European Union (EU) facilitate compatibility between digital platform services, such as cloud providers and digital intermediaries. The intention is to increase supply and demand by creating and promoting an environment that encourages businesses and individuals to choose and use the services that suit their needs. This vision requires that companies and citizens can switch easily and quickly between different providers according to their changing requirements. The Digital Markets Act can be used to help companies segment their needs and collaborate with the right partners, thus reducing the gatekeeping and lock-in effects that hinder innovation. In addition, after much civil society campaigning, the DMA now imposes a very specific in-

teroperability obligation on messaging/calling services (known in EU law as Number Independent Interpersonal Communications Services). Such services are required to provide a technical 'interface' (probably public Application Programming Interfaces or APIs) to interested competitors for specific 'basic functions'. Initially, these would be one-to-one text conversations, and later group discussions and group–individual voice and video calls. By implementing these measures, the EU can promote a competitive market that fuels innovation, creating new opportunities for businesses and individuals, while driving economic growth. The role of governments as well as local administrations is important in attracting private investment to build infrastructure to provide homes and businesses with full-fibre and gigabit-capable digital connectivity.

- Increasing the amount of data leveraged is very important for governments and public sector organisations. A vast amount of data is collected through automated processes, including sensors, and thus far too much for humans to manage in the old fashioned way. This means that AI systems will become more crucial in identifying patterns. At the same time, too much data is in proprietary data sets so the EU should make every effort to ensure it is secure, while also allowing scrutiny, transparency, fairness and accountability.

A culture of investment, growth and risk

Technology is often seen as part of a global race. And Europe is regarded as lagging behind. In the particularly important military domain, China and the United States are competing to develop AI capabilities that will transform warfare. The capacity of AI systems, for example, to analyse surveillance imagery, medical records, social media behaviour and even online shopping habits will allow what technologists call 'micro-targeting', attacks with drones or precision weapons on key combatants or commanders, even if they are nowhere near the front lines. Ukraine's crafty utilisation of technolo-

gy to counter Russia's invasion is further igniting this rivalry.[59] This high-stakes tech battle potentially puts those who dominate areas such as AI and autonomous weaponry in pole position. 'Being the frontrunner in the software aspect of this strategic competition is crucial. It regulates everything, extending from weather forecasting, climate change simulations, new-age nuclear weapon trials, to the invention of extraordinary new weapons and materials that could offer the upper hand on the battlefield and beyond.'[60] The report continues: if America fails to act, it 'could see a shift in the balance of power globally, and a direct threat to the peace and stability that the United States has underwritten for nearly 80 years in the Indo-Pacific'. 'This is not about the anxiety of no longer being the dominant power in the world; it is about the risks of living in a world in which the Chinese Communist Party becomes the dominant power.'[61]

The argument is that the EU seems to be lagging behind in the tech race unfolding between the United States and China, in which a number of other countries are also playing a major role, such as India. The EU's detractors often argue that a less regulated approach spurs innovation and cite Silicon Valley as a clear example. The argument is that private sector innovation has been allowed to thrive in America thanks to economic freedom, lack of controls, strong venture capital and a more conducive approach to risk. Having said that, China's centralised and controlled approach is also often cited as the reason for China's technological leadership. On one hand, a lack of control is supposed to spur creativity, but on the other, total control enables massive data collection and strategic direction.

Of course this is a simplified narrative, but it does reflect the thinking among policymakers, business and the general population. The vociferous reaction to the EU's AI Act reflects such views, with

59 Russia's military hit by high-ranking losses in Ukraine, Reuters https://www.reuters.com/world/europe/russias-military-hit-by-high-ranking-losses-ukraine-2022-03-23/.

60 In the US-China AI contest, the race is on to deploy killer robots, Reuters, https://www.reuters.com/investigates/special-report/us-china-tech-drones.

61 Ibid.

claims that AI regulation will inevitably hinder innovation and solidify Europe's position as an eternal laggard in the global technology race.

But is it true?

To some extent, it is. Europe is not home to any of the large technology companies that dominate the digital landscape. Nevertheless, we are now seeing efforts in most countries – from China to the United States – to rein in large companies through robust antitrust measures and demands for transparency with regard to how they operate and serve their customers.

But we need a clear idea of why Europe is lagging behind and stumbling in the global race. To get it, we must first debunk the myth that the success of large US corporations depends on a combination of deregulation and entrepreneurialism. Actually, it is the quite the opposite. It is governments, not venture capitalists and tech visionaries, that have fuelled innovation. Every major technological advancement in recent decades has been funded by the state. Mariana Mazzucato has traced the origins of technological breakthroughs over recent years and outlines how, for example, it was the Defense Department that spurred research in the parts of smart phones that make them smart. And it was the US Department of Energy that handed a grant to Tesla to develop battery technologies and solar panels. Finally, the National Science Foundation supported the creation of Google's search algorithm.

And what about Europe? Europe hasn't always struggled with innovation. In the early 2000s, Finland's Nokia led the mobile phone industry, and at around the same time, Skype made its way emerged from Estonia to dominate the nascent video-messaging market. In the space of a decade or two, however, these companies – and many others like them – have been supplanted by rivals from other countries.

But there is more to it. While the EU has provided research and development funding, transparency has lagged behind, thus making it impossible to trace where the money has gone and what the re-

turns are. Coupled with that, European firms often lack access to the capital needed to scale up, meaning that they often have to look to China or the United States for further growth opportunities. Skype is a case in point: although the firm was founded in Europe, it wasn't too long before the company accepted an $8.5bn (€7.6bn) takeover bid from Microsoft.

So what needs to happen?

- Rethinking funding. Horizon Europe, the EU's €100bn R&D programme, was launched in 2021 to support the growth of digital skills and the development of the businesses that rely on them. There are two things with EU funding schemes that need fixing urgently. Though. First, it is arguable that the Horizon programme is not as forward thinking as it should be, in the sense that it does not favour moonshot programmes, which require a long-term approach, close supervision and the ability to look ahead strategically. Second, the handling of these programmes is not transparent enough, on top of being too short-term.
- In addition to more transparency, the EU needs much more private investment in AI. In 2016, Europe devoted only 2.4–3.2 billion euros in investment funds, whereas Asia invested 6.5–9.7 billion euros and North America invested 12.1–18.6 billion. 36 Private equity and venture capital firms have accounted for 75 per cent of AI-related deals in Europe in the past ten years.
- Simplifying European funding institutions: Institutions such as the EIC and the European Investment Bank play a major role. The EIC provides both equity and grant financing, while the EIB provides venture credit. However, these institutions need to raise their game and simplify access and procedures. The burden of compliance is reported as a major obstacle by many deep-tech startups: 'some companies hire dedicated em-

ployees or contract with consulting agencies to manage the grant processes, a significant drain on the actual investment.'[62]

- Invest in the creation of scale-ups, in other words entrepreneurial ventures that 'are entering a growth phase where they seek significant market penetration'. One proposal is to establish a EU sovereign tech fund and an EU sovereign green tech fund to address the scale-up finance gap to develop the venture capital (VC) financing system. The proportion of later-stage investment in total venture capital funding was 81 per cent in the United States, but only 74 per cent in the EU in the first semester of 2021.[63] This funding gap has – to some extent – been filled by foreign investors, which account for a significant proportion of investments in EU scale-ups (73.1 per cent according to Tech.eu, 2019[64]) with potential negative consequences in terms of relocation of jobs, knowledge, revenue streams and talent.[65]
- Pushing the private sector to do more: as we discussed above, there is a false mythology that the private sector spurs innovation, and the public sector hinders it through red tape. We have seen that this is not true. The examples of US innovation fuelled by government institutions eloquently describe the necessary partnership between the public and private realms. Europe has a vibrant early stage start-up ecosystem. Too often, these startups cannot find the capital they need, and they end

62 Can Europe Create Its Own Deep-Tech Giants?, BCG, https://www.bcg.com/publications/2022/how-can-europe-build-deep-tech-leaders.

63 Quas, Anita, Mason, Colin, Compañó, Ramón, Testa, Giuseppina, Gavigan, James P. (2022): The scale-up finance gap in the EU: causes, consequences, and policy solutions, in: *European Management Journal*, https://doi.org/10.1016/j.emj.2022.08.003.

64 Tech.eu (2019): Blooming late: the rise of late-stage funding for European technology scale-ups, https://tech.eu/wp-content/uploads/woocommerce_uploads/2019/05/Blooming-Late_FA.pdf.

65 Braun, Reiner, Weik, Stefan and Achleitner, Ann-Kristin (2019): Follow the Money: How Venture Capital Facilitates Emigration of Firms and Entrepreneurs in Europe (5 July), SSRN: https://ssrn.com/abstract=3415370 or http://dx.doi.org/10.2139/ssrn.3415370.

up being purchased by larger companies, often from outside Europe. While EU public sector funding mechanisms need to be reshaped and their transparency enhanced, private investment also needs to smarten up.

Creating sustainable progress

To create long-term sustainability, Europe must look at technological progress through the paradigm of sustainability. This involves:

- Individual sustainability: technology must enhance, not undermine individual rights and standing in the world. This means protecting privacy and autonomy in the digital ecosystem, and using technology to enhance people's democratic participation and opportunities in life.
- Societal sustainability: we have seen how modern societies run on code. Whether we buy something online or in a store, borrow a book from the library or make an appointment at the doctor, we will almost always be interacting with a system powered by software. The complexity of code keeps increasing and with that the power of a handful of companies and the challenges for consumers and citizens. In the previous chapter we saw how the EU is tackling the first aspect. However, that will not suffice unless citizens use and trust the systems that are created. To a large extent, data is people – and while we don't want valuable data to go to waste (any more than we want to waste water) misuse of data eats away at trust and puts people off from relying on technological tools. So often daily life cannot be conducted without such tools, so people are put under the strain of being forced to use systems that they do not trust. This is not healthy in the long run.
  Building trust is therefore essential, and that requires that governments:
  - ensure that systems undergo due diligence;
  - reward innovative systems that champion privacy, data protection and human rights;

  - invest in research into privacy-enhancing technologies, and their availability;
  - enable citizens and consumers to understand the technology that they are using;
  - champion individuals' recourse to redress when a technological tool discriminates against them;
  - promote digital awareness, fight exclusion and digital poverty;
  - recognise that access to online services may lock certain groups of people out, especially if they are elderly or have disabilities.
- Environmental sustainability: Technology's potential role in tackling climate change is widely recognised but the sustainability of technology itself is often overlooked. For example, AI can have a dramatically negative impact on carbon footprints, an externality that sadly continues to be overlooked. Training a single large AI system has a huge environmental impact: hundreds of thousands of kilos of CO_2 are emitted, comparable to the lifetime carbon emissions of several cars.[66] The authors of *Green AI*[67] note that 'the computations required for deep learning research have been doubling every few months, resulting in an estimated 300,000 x increase from 2012 to 2018'. They also point out that 'ironically, deep learning was inspired by the human brain, which is remarkably energy efficient'. Green AI is one of the new initiatives that have suggested moving from the sole focus on AI for sustainability (namely, how AI can help sustainability) towards sustainable AI, and that means taking energy efficiency as an evaluation criterion for research, alongside accuracy and related considerations. They propose reporting the financial cost or 'price tag' of developing, training and running models to provide baselines for the

66 Strubell, Emma, Ganesh, Ananya and McCallum, Andrew (2019): Energy and policy considerations for deep learning in NLP, https://arxiv.org/abs/1906.02243.

67 Schwartz, Roy, Dodge, Jesse, Smith, Noah A. and Etzioni, Oren (2019): Green AI, https://doi.org/10.1145/3381831.

investigation of increasingly efficient methods. Others[68] suggest the introduction of SECure certificates which, if properly done and perhaps leveraged through solid procurement rules, would promote adherence to specific aspects of environmental sustainability. For example, they include the use of Federated Learning that, in addition to enormous benefits from a privacy and data protection standpoint, also has the 'second-order benefit of enabling computations to run locally, thus potentially decreasing carbon impacts if the computations are done in a place where electricity is generated using clean sources'.[69]

Above all, there is no doubt that Europe must invest in green technology, which uses science and technology to protect the world's natural resources and mitigate the negative environmental impact of human activity.

In conclusion, while the EU needs to take a multi-faceted approach to digital policy, a number of key considerations loom large. It must be recognised that technology is crucial to global policymaking and diplomacy, as well as growth. There is no doubt that the war in Ukraine has brought all this to the fore. The EU has been very vocal in supporting Ukraine on cyberdefence, for example. In today's world, there is no geopolitical dimension that does not involve technology. Technology is often the battlefield where a lot of complex geopolitical issues are anticipated and go on display.

For this reason, building a competitive Europe requires a 360 degree approach to technology that starts with standing tall in a complex supply chain. That is the way forward – isolation, technological nationalism or data protectionism are totally inadequate.

68 Gupta, Abhishek (ND): Social and Environmental Certificate for AI Systems, https://branch.climateaction.tech/issues/issue-2/secure-framework/.

69 See note 67.

Rethinking the relationship between society and technology

In the previous chapter, we looked at how government agencies use algorithms to automate decisions on welfare provisions, criminal justice, health care and many other contentious aspects of social life. Eubanks contends[70] that governments, by circumventing the principle of inclusion, manage to maintain the ethical detachment they need to make unpopular decisions on issues such as the distribution of food and housing and the breaking up of families. We can take the example of 'robodebt' in Australia to illustrate the fallout from an algorithm's proneness to making brutal judgments. In 2016, several Australian social security recipients started to receive notifications of so-called debts, dictated by a government agency's debt-collection algorithm, instituted to improve collection efficiency. However, the algorithm was defective and became infamous as 'robodebt'. The people affected vehemently contested these decisions, using the hashtag #notmydebt, sharing personal accounts on a dedicated website, and eventually instigating a successful class action. The court ruling was in their favour and led to the payment of AU$1.2 billion in compensation for unjustly assigned debts. Further inquiries into the incident by parliamentary and Commonwealth ombudsmen investigated the democratic boundaries of algorithm usage and automated decision-making. **They concluded that this approach to debt collection violated the standards of transparency and procedural fairness. People were unable to discern the logic underlying the decisions and so were unable to understand them.**

Based on a data-driven and dangerously simplistic approach to dealing with the complexities of public life, creeping dependence on algorithms is progressively eroding the democratic foundation of our societies. It is becoming increasingly more difficult to scrutinise algorithmic decision-making. We have already seen how AI decision-making can lock people of out of essential services. Here,

70 Eubanks, V. (2018): *Automating inequality: How high-tech tools profile, police, and punish the poor*, 1st ed., St Martin's Press.

the focus is how the 'algorithmic society' lacks democratic controls and opportunities for public deliberation. While the GDPR and the EU AI Act impose some controls on these systems, there is no doubt that the looming 'algocracy' reflects an unthinking deference to AI experts, whose hegemony risks sidelining public deliberation and politics.

A progressive approach to technology should focus on establishing clear paths for public participation in establishing a logical separation between humans and algorithms that benefits society.

Digital literacy and tech inequality

Almost a year after OpenAI introduced the chatbot ChatGPT, there has been a surge of competition among companies to create potent generative AI systems. With each new iteration, these systems are becoming more capable, gradually encroaching on human abilities. By generating text, visuals, videos and even software, based on human inputs, these AI solutions are helping to make information more easily understandable and to accelerate technological advance. However, they also come with potential hazards. AI-created content has the ability to inundate the internet with false information and convincingly fabricated 'deepfakes', videos that feature realistic and practically indistinguishable artificial faces and voices. In the long term, these problems could undermine trust among individuals and in political leaders, news outlets and institutions.

It is crucial that the EU combat this. As previously mentioned, the EU AI Act demands transparency, including disclosure of the fact that content is AI-generated and publication of summaries of copyrighted data used for training AI systems. US President Joe Biden obtained voluntary commitments from seven leading tech companies 'to manage the risks posed by Artificial Intelligence (AI) and to protect Americans' rights and safety'. Digital 'watermarks' that identify the origins of a text, picture or video might be one such mechanism.

However, it is still unclear what protections will be needed in the long term to safeguard our democratic viability and trust in our institutions. One thing is certain, however, and that is that for Europe to

harness the value of this technology it is crucial that it also invest in digital literacy. This involves educating Europeans against the harms and steering them towards active participation in the democratisation of tech processes, as previously discussed. Secondly, digital literacy fosters responsible use, which in turn is crucial to generating demand.

A recent WHO report[71] showed that just over half the countries in the region have developed policies for digital health literacy and have implemented a digital inclusion plan. This issue must be addressed.

It is also worth noting that the connection between digital skills and income inequality is not straightforward. As a recent study found,[72] boosting workers' digital skills may help to reduce inequalities in the higher-income brackets. On the flip side, there's a direct correlation between advanced digital skills in the workforce and economic disparity for low-income groups. That implies that an escalation in digital proficiency parallels greater inequality among the less affluent. For this reason, educational programmes must be established or enhanced for those with lower skills to minimise the threat posed by burgeoning digitalisation, which could adversely affect equality and societal harmony. Adopting a mix of policies that not only support digitalisation initiatives but also counteract the potentially negative social consequences of digitalisation is one way of tackling societal issues arising from the unequal distribution and use of ICTs.

It is fair to say that the concentration of power in large technology companies (which AI is likely to exacerbate) and the broader digitalisation of our lives, while bringing some enormous advantages (and convenience), are also creating a great divide between the haves and

71 WHO, Digital health divide: only 1 in 2 countries in Europe and central Asia have policies to improve digital health literacy, leaving millions behind, https://www.who.int/europe/news/item/05-09-2023-digital-health-divide--only-1-in-2-countries-in-europe-and-central-asia-have-policies-to-improve-digital-health-literacy--leaving-millions-behind.

72 Consoli, Davide, Castellacci, Fulvio and Santoalha, Artur (2023): E-skills and income inequality within European regions, in: *Industry and Innovation*, 30:7, 919–946, https://doi.org/10.1080/13662716.2023.2230222.

the have-nots. In other words, the digitalisation of everything is distorting our economic landscape. Education and upskilling are certainly important means for addressing this (as discussed above), as is technology itself. However, there is clearly a need to democratise the benefits of the Fourth Industrial Revolution in the face of the concentration of power (and wealth) in the hands of large corporations.

We have already discussed how the EU is tackling the issue of corporate power through a suite of legislative tools aimed at ensuring, among other things, better competition, better use of data for the public good and better transparency for users.

But ultimately, the crux of the matter is how we manage to reshape the wider architecture of production, finance and public private institutions in a way that strikes a different balance between these stakeholders (as Mariana Mazzucato calls these three pillars). This requires establishing an alliance in which companies invest more in R&D for future innovation in areas such as green tech, governments play an active role in directing growth so that it is inclusive and sustainable, and citizens participate through deliberation and civic engagement. Europe could and should be the catalyst in finding ways of making the digital transition work for people and society.

Glossary

Algorithmic Bias
A phenomenon that occurs when an algorithm or a system produces unfair or discriminatory outcomes or decisions based on the data, design, or implementation, affecting individuals or groups based on their protected attributes, such as race, gender, age, or religion.

Artificial Intelligence
The field of computer science that aims to create systems or machines that can perform tasks that normally require human intelligence, such as reasoning, learning, decision making, natural language processing, or vision.

Blockchain
A distributed system that records and verifies transactions using cryptography and consensus mechanisms, creating a secure and immutable ledger that can be shared among multiple parties.

Computer Vision
A branch of artificial intelligence that deals with the analysis and understanding of visual information, such as images or videos, using methods such as face recognition, object detection, segmentation, or scene understanding.

Data Sharing
A practice that involves making data available and accessible to other individuals, organizations, or systems for various purposes, such as research, collaboration, innovation, or public service. Cross-border data sharing is often considered as a geopolitical matter as it relates to technology sovereignty.

Deep Learning
A subfield of machine learning that uses neural networks with multiple layers of processing units to learn complex patterns or features from large amounts of data.

Deepfakes
A term that refers to synthetic media, such as images, videos, or audio, that are generated or manipulated by artificial intelligence, especially deep learning, to create realistic but false representations of people or events. Deepfakes pose ethical and social challenges related to trust, privacy, consent, and misinformation.

Digital Advertising
A form of marketing and communication that uses digital platforms and channels, such as websites, social media, email, or mobile apps, to deliver and display promotional messages, images, videos, or audio to target audiences.

Digital Inclusion
A term that refers to the efforts and initiatives to ensure that everyone has equal access and opportunity to use and benefit from digital technologies and services, regardless of their socio-economic status, location, education, or ability.

Frontier AI
A term that refers to the cutting-edge research and applications of artificial intelligence that aim to achieve human-like or superhuman capabilities, such as artificial general intelligence, artificial creativity, or artificial consciousness.

Gig Economy
A term that describes a labour market that consists of independent contractors, freelancers, or temporary workers who perform short-term or on-demand tasks or services for various clients or platforms, such as Uber, Airbnb, or Fiverr.

Interoperability
A property that allows different systems, devices, or applications to communicate and exchange data and information, using common standards, protocols, or formats. Interoperability facilitates collaboration, integration, and compatibility among various actors and sectors in the digital ecosystem.

Machine Learning
A branch of artificial intelligence that focuses on creating systems or machines that can learn from data and improve their performance without explicit programming or human intervention.

Metaverse
A term that describes a hypothetical virtual reality where people can interact with each other and with digital environments and content, using various devices and platforms.
Microtargeting
A technique that uses data analysis and algorithms to segment and identify specific groups or individuals based on their characteristics, preferences, or behaviours, and to tailor and deliver customized messages or content to them. Microtargeting presents challenges related to surveillance, disinformation and manipulation.
Quantum Computing
A field of computer science that uses the principles of quantum mechanics to create and manipulate quantum bits or qubits, which can store and process information in superposition and entanglement states, enabling exponential speedup and parallelism for certain problems.
Smart City
A concept that applies digital technologies and data-driven solutions to urban planning and management, aiming to improve the efficiency, sustainability, and livability of cities. Smart city initiatives may involve areas such as transportation, energy, water, waste, security, health, education, or governance.
Technology Sovereignty
A concept that refers to the ability and right of a nation or a region to determine its own policies and practices regarding the development, deployment, and governance of technology, especially in relation to data protection, cybersecurity, digital infrastructure, and innovation.
Venture Capital
A form of financing that provides funds to start-ups or small businesses that have high growth potential, but also high risk of failure. Venture capital investors usually receive equity or ownership shares in the companies they fund, and may also offer guidance, mentoring, or networking opportunities.
Virtual Reality
A technology that creates and simulates an immersive and interactive three-dimensional environment that users can experience and

manipulate through devices such as headsets, controllers, or gloves. Virtual reality can be used for various purposes, such as entertainment, education, training, or therapy.

5G

A fifth-generation mobile network technology that offers faster speeds, lower latency, higher capacity, and more reliability than previous generations. 5G enables new applications and services in various domains, such as the Internet of Things, cloud computing, artificial intelligence, and augmented reality.

List of abbreviations

AI	Artificial Intelligence
AIA	AI Act
AR	Augmented Reality
COE	Council of Europe
DMA	Digital Markets Act
DSA	Digital Services Act
FFDR	Free flow of non-personal data in the European Union Regulation
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IoT	Internet of Things
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
OECD	Organization for Economic Co-operation and Development
R&D	Research and Development
TCC	Trade and Technology Council
UN	United Nations
VC	venture capital
VR	Virtual Reality
WWW	World Wide Web

Tech policy leaders in Europe

Many people have contributed to the development of tech policy in Europe. Here, only a short selection are listed.

Peter Altmaier: Federal Minister for Economic Affairs and Energy in Germany.

Brando Benifei: MEP (S&D, Italy).

Tim Berners-Lee: The inventor of the World Wide Web and the director of the World Wide Web Consortium, which oversees its development.

Abeba Birhane: Cognitive science researcher and a PhD candidate at University College Dublin.

Thierry Breton: European Commissioner for Internal Market.

Francesca Bria: Digital policy expert and a co-founder of the Decode project, which aims to give people more control over their personal data.

Mayte Ledo Turiel: Spanish Secretary of State for Digitalization and Artificial Intelligence.

Kate Crawford: Leading scholar of the social implications of artificial intelligence. She is a Senior Principal Researcher at Microsoft Research New York.

Virginia Dignum: Professor of social and ethical artificial intelligence at Umeå University in Sweden.

José van Dijck: Media scholar and a distinguished university professor at Utrecht University.

Tristan Harris: Former design ethicist at Google and a co-founder of the Center for Humane Technology.

Věra Jourová: Vice President of the European Commission for Values and Transparency.

Jaron Lanier: Pioneer of virtual reality and a critic of digital culture.

Marianne Mazzucato: Economist and a professor at University College London, where she directs the Institute for Innovation and Public Purpose.

Phoebe V Moore: Sociologist and associate professor of political economy and technology at Leicester University.

Evgeny Morozov: Writer and researcher who critiques the political and social implications of digital technologies.

Paul Nemitz: Lawyer and a director for fundamental rights and rule of law at the European Commission.

Cédric O: French Secretary of State for Digital Affairs.

Aza Raskin: Designer, entrepreneur, and co-founder of the Center for Humane Technology.

Johnny Ryan: Privacy and digital rights activist who campaigns against online surveillance and data exploitation.

Marietje Schaake: Former member of the European Parliament and a current international policy director at Stanford University's Cyber Policy Center.

Lucilla Sioli: Director for Artificial Intelligence and Digital Industry in the European Commission.

Dragoș Tudorache: MEP (Renew Europe, Romania).

Margrethe Vestager: Executive Vice President of the European Commission for A Europe Fit for the Digital Age.

Roberto Viola: Director-General of DG CONNECT in the European Commission.

Axel Voss: MEP (EPP, Germany).

Meredith Whittaker: President of the Signal Foundation and co-founder of the AI Now Institute.

Shoshana Zuboff: Scholar, author, and activist who coined the term "surveillance capitalism" to describe the new economic order that exploits personal data for profit.

Ethan Zuckerman: Writer, educator, and activist who focuses on the impact of digital media on the public sphere.

To explore further

Margaret Boden, Joanna Bryson, Darwin Caldwell, Kerstin Dautenhahn, Lilian Edwards, Sarah Kember, Paul Newman, Vivienne Parry, Geoff Pegman, Tom Rodden, Tom Sorrell, Mick Wallis, Blay Whitby, and Alan Winfield. 2017. Principles of robotics: regulating robots in the real world.

Stanford University, Rethinking Privacy in the AI Era , White Paper, https://hai.stanford.edu/sites/default/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf

France Digitale, AI Actg ,February 2024 https://media.francedigitale.org/app/uploads/prod/2024/02/01162803/Compliance-AI-Act-Feb-24.pdf

Peter Drahos, Survival Governance: Energy and Climate in the Chinese Century (Oxford University Press, 2021)

Chris Miller, Chip War, The Fight for the World's most critical technology, 2022

Daniel Susskind, A world without work, 2020

Bergemann, B. (2018). The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection. In M. Hansen, E. Kosta, I. Nai-Fovino, & S. Fischer-Hübner (Eds.), Privacy and Identity Management. The Smart Revolution (Vol. 526, pp. 111–131). Springer International Publishing. https://doi.org/10.1007/978-3-319-92925-5_8

Birhane, A., & Guest, O. (2021). Towards Decolonising Computational Sciences. Kvinder, Køn & Forskning, 2, 60–73. https://doi.org/10.7146/kkf.v29i2.124899

Bradford, A. (2024). The False Choice Between Digital Regulation and Innovation. Northwestern University Law Review, 118 (2). http://dx.doi.org/10.2139/ssrn.4753107

Buolamwini, J. (2016). The Algorithmic Justice League [Medium Post]. MIT Media Lab. https://medium.com/mit-media-lab/the-algorithmic-justice-league-3cc4131c5148

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings

of Machine Learning Research, 81, 1–15. http://proceedings.mlr.press/v81/buolamwini18a.html
Citron, D. K. (2014). Hate crimes in cyberspace. http://www.dawsonera.com/depp/reader/protected/external/AbstractView/S9780674735613
Gebru, T., & Torres É. P. (2024). The TESCREAL bundle: Eugenics and the promise of utopia through artificial general intelligence. First Monday, 29(4). https://doi.org/10.5210/fm.v29i4.13636
Malgieri, G., & González Fuster, G. (2021). The Vulnerable Data Subject: A Gendered Data Subject? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3913249
Mantelero, A. (2016). Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection. Computer Law & Security Review, 32(2), 238–255. https://doi.org/10.1016/j.clsr.2016.01.014
Matzner, T. (2014). Why privacy is not enough privacy in the context of "Ubiquitous Computing" and "Big Data." Journal of Information, Communication and Ethics in Society, 12(2), 93–106. https://doi.org/10.1108/JICES-08-2013-0030
Mejias, U. A., & Couldry, N. (2019). Datafication. Internet Policy Review, 8(4). https://doi.org/10.14763/2019.4.1428
Wiener, A., Börzel, T. A., & Risse, T. (Eds.). (2018). European integration theory (Third edition). Oxford University Press.
World Economic Forum. (2018). The Global Gender Gap 2018 [Report]. World Economic Forum. https://www.weforum.org/reports/the-global-gender-gap-report-2018
Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, 30, 75–89. https://doi.org/10.1057/jit.2015.5
Meredith Broussard, Artificial Unintelligence: How Computers Misunderstand the World, MIT Press: Cambridge, Mass., 2018.
Mary L. Gray and Siddharth Suri, Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass, Houghton Mifflin Harcourt: Boston, 2019.

Reviews

Dr. Krzysztof Gawkowski, Deputy Prime Minister of Poland and Minister of Digital Affairs

Ivana Bartoletti is an incredibly knowledgeable author. In this book, she skilfully introduces the readers into the meanders of digitalisation – while showing the great potential that this incomparable transformation could have. Bartoletti informs and instructs, but above all identifies the choices that humanity is facing. These are first and foremost political, and she insists that they must be coherently faced globally, by the EU and on the national levels. Consequently, Bartoletti points to what has been done and how to move on, showing the progressive path forward and proposing a complementary narrative. This all makes this Primer a must read.

Miapetra Kumpula-Natri, S&D MEP, Vice President EP Delegation for relations with the United States

The book provides an excellent view of the current digital transformation and the societal tensions related to it. Bartoletti uniquely presents clear descriptions of technological developments from data to AI and analysis of digitalisation's impact on work, education, and social life offers though - provoking and insightful perspectives essential for all progressive policymakers. She offers useful avenues of change by rethinking the relationship between society and technology, and by addressing issues like sustainable progress, digital literacy, and tech inequality, which should guide the building of a digital union based on European values.

Brando Benifei, S&D MEP

Ivana Bartoletti, a prominent advocate for digital rights in the European context, offers readers a comprehensive exploration of the key features and dilemmas of the digital landscape. With a forward-thinking approach, Bartoletti navigates from the inception of the internet to the emergence of blockchain, 5G, artificial intelligence and beyond.

Addressing the intricacies surrounding new technologies and social media, from recent advancements to privacy concerns, digital sovereignty and safeguarding fundamental rights, this primer tackles complex subjects with remarkable clarity. It serves as an accessible resource for anyone seeking to understand the significant political divides inherent in the digital realm – challenges that will shape our future. Bartoletti's work underscores the importance of striving for a European model of a digital society that leaves no one behind.

Sofie Amalie Stage, YES Secretary General *(Young European Socialists)*

With the primer "A Digital Union based on European Values" the reader gets a concrete and to the point introduction to tech and digitalisation policy in Europe. It shows not only how current policy measures such as GDPR, DMA, DSA and the recent AI act contributes to strengthened rights of the consumers, but also elaborates on the ongoing policy development debate within Europe, focusing on factual circumstances and the inclusion of European Values of freedom, democracy and human rights. The technological development is only sprinting faster, and this primer gives an outstanding base knowledge on the matter, ensuring your ability to jump into the highly relevant debate on technology and digital transition including the fast-developing Artificial Intelligence and how we make sure technology is a positive asset to the human experience, and does not become a threat. Ivana Bartoletti's ability to simply explain complicated matter makes the book a perfect read for anyone new to politics and interested to delve into the world of policy development, but also an asset for anyone currently working in politics, but curious on the complicated topic of tech policies.

Dr. Fabian Ferrari, Postdoctoral Researcher at Utrecht University

Ivana Bartoletti's primer presents a holistic perspective on our digital landscape dominated by Big Tech. Essential reading for those eager to shape digital policy, her work provides not only a solid foundation of key terms, but also a guide to envision new progressive futures. But in order to change this status quo, such as by building digital public infrastructure or rethinking funding institutions, one must first understand it. Bartoletti's primer equips progressives with a clear compass to navigate a world shaped by AI and digital platforms.

Dr. Dimitris Tsarouhas, Professor of International Affairs, Global Fellow, The Woodrow Wilson Center for International Scholars, Member of FEPS Scientific Council

The Fourth Industrial Revolution is transforming modern society one step at a time, from service delivery and data flows to entertainment access and cyber security. It constitutes one of the greatest challenges of our time, with governments trying to keep up with the pace of technological innovation promulgated by Big Tech, and citizens enjoying the benefits of convenience that tools such as AI bring, while worrying about its implications for their jobs and privacy.

The new FEPS primer is authored by one of the most prominent experts on the field, Ivana Bartoletti, and it manages to serve three functions simultaneously. First, it *educates* through a *tour de force* on the technological evolution of our time and how it has come about through an accessible and straightforward first part. Second, it *analyses* where we find ourselves today, in Europe and across the world, in terms of the pace of technology and the effects of the digital revolution on the public and private sphere. Third, Bartoletti *suggests concrete* ways through which the EU can emerge on top of this gigantic, transformative wave engulfing all of humanity.

Conscious of the deleterious effects that the large concentration of power in the hands of a few large tech companies, not least in terms of widening the gulf between the digital haves and have-nots, she praises the capacity of the EU to regulate (the "Brussels effect") and set standards for the world by ensuring transparency for users and

breaking down monopolistic structures. At the same time, however, her message of reform is clear: Europe needs to do a lot more to incentivise European firms to invest in R&D for innovation purposes, to stand its ground in the heightened global competition on AI, and promote better data use serving the public good. A Luddite approach to the new era, she warns, will only harm the capacity of Europe to embrace the era of inclusive and sustainable growth it aspires to. I sincerely hope that her powerful message will reach a wide audience, not least among policy-makers and regulators.

About the Author

Ivana Bartoletti is a leader in the field of privacy, data protection and responsible technology. She is an expert on AI and gender rights at the Council of Europe, and is a Cybersecurity and Privacy Executive Fellow at Virginia Tech. She has extensive experience in shaping privacy policies, strategies and programmes for large organizations undergoing digital transformation, cloud and automation. She received the Privacy Leader of the Year Award in London in 2022. Ivana is also the founder of the influential Women Leading in AI network, and a former chair of the Fabian Society.

The FEPS Primer Series

Following a decade of polycrisis that followed the great recession of 2009, progressive political thinking and practice in Europe needs a reconstruction. This FEPS Primer book series was launched to serve the creation of this new synthesis, connecting long established values of the European socialist and social democratic traditions with the lessons and innovations of the current experience.

Primers are booklets written with an educational purpose, to help new (typically young) audiences enter specific thematic fields, which can be diverse (in this case social science, politics, and policy). Accessible language is important, together with illustrations that highlight key elements of the content. The main text is always accompanied by a glossary as well as a section of recommended further reading.

The FEPS Primers are parts of a broader effort: the Foundation endeavours to raise progressive political education in Europe to a new level. Our volumes aim to provide useful analysis, instruction, and orientation for several years after publication. Some of them may well be considered 'must reads' for all those aspiring to play an active role in European politics at any level.

Our authors are not only recognised experts, but also active participants in political and policy debates, representing a diversity of European nations and career paths. However, they are connected by sharing the values and objectives of the progressive political family and concerns for the future of European societies, as well as sustainability and social cohesion as common goals.

The FEPS Primer series is edited by an Editorial Board. We keep in view the key current issues of the European Union, with a focus on critical discussion points that will influence the work of social movements as well as governance at various levels in the coming decade. We hope the selection of topics and the contributions of our distinguished authors will spark the interest of those participating in progressive political education, and also appeal to a wider readership.

Dr László Andor
FEPS Secretary General

"Ivana Bartoletti is an incredibly knowledgeable author... she points to what has been done and how to move on, showing the progressive path forward and proposing a complementary narrative. This all makes this Primer a must read."

Dr. Krzysztof Gawkowski
(Deputy Prime Minister of Poland and Minister of Digital Affairs)

"The book provides an excellent view of the current digital transformation and the societal tensions related to it. She offers useful avenues of change to build a digital union based on European values."

Miapetra Kumpula-Natri
(S&D MEP, Vice President EP Delegation for relations with the United States)

"A comprehensive exploration of the key features and dilemmas of the digital landscape. This primer tackles complex subjects with remarkable clarity."

Brando Benifei
(S&D MEP)

"This primer gives an outstanding base knowledge on the matter, ensuring your ability to jump into the highly relevant debate on technology and digital transition... A perfect read for anyone new to politics but also an asset for anyone currently working in politics."

Sofie Amalie Stage
(YES Secretary General [Young European Socialists])

"Essential reading for those eager to shape digital policy. Bartoletti's primer equips progressives with a clear compass to navigate a world shaped by AI and digital platforms."

Dr. Fabian Ferrari
(Postdoctoral Researcher at Utrecht University)

ISBN 978-3-8012-3108-8

9 783801 231088

www.dietz-verlag.de