trigger
Trends In Global Governance and Europe's Role

D4.6 WP4 final report

WP4 Governance and technologies: interrelations and opportunities

Grant Agreement n° 822735, Research and Innovation Action

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

TRIGGER

TRends In Global Governance and Europe's Role

Deliverable number:	
Deliverable name:	D4.6 WP4 final report
WP / WP number:	WP4 Governance and technologies: interrelations and opportunities
Delivery due date:	M24
Actual date of submission:	M28/ March 2021
Dissemination level:	Public
Lead beneficiary:	EPFL
Contributor(s):	Marie-Valentine Florin Aengus Collins
Reviewers(s):	Gianluca Misuraca Carlo Sessa Jonathan Zysman

Changes with respect to the DoA

Due date changed in amendment submitted in March 2021, from M23 to M28

Dissemination and uptake

Public

Evidence of accomplishment

Report

Content

Introduction

The focus of WP4 on "governance arrangements and regulatory frameworks" relating to emerging technologies (and emerging applications of existing technologies) has become increasingly important. Over the course of the TRIGGER project's duration, digital technology has become an even more central feature of the global governance landscape. Among other things, this is reflected in the priorities of the current European Commission, whose focus on geopolitical developments and on "technological sovereignty" (for further discussion, see D4.5) represents a clear aspiration to shape regional and global patterns of technology governance in order to protect European interests and values. This is in line with evolving priorities across the EU, as exemplified by the fact that the Portuguese presidency of the Council in the first half of 2021 highlighted "strategic autonomy" as one of its priorities (Portuguese Presidency of the Council of the European Union, 2021).[1]

The purpose of this final report from WP4 is two-fold. Part 1 will briefly review the work carried out in this work package. This comprises three reports focused on global governance in specific technology areas (open standards and open-source software in D4.1; distributed ledger technologies in D4.2; and artificial intelligence/machine learning in D4.3), as well as two more thematic assessments of the EU's role in the changing technology governance landscape (D4.4 and D4.5). In Part 2, this report will pull together a number of strands from this earlier work in an assessment of what lies ahead for the EU in the area of technology governance, with a view to identifying (in section 2.4) a series of principles or recommendations that should shape the EU's future activities in this field.

In developing this forward-looking part of the report, we will draw on other TRIGGER work insofar as it helps to clarify the nature of the choices about technology governance that the EU will have to make. This includes the four scenarios that have been developed in WP5 (see D5.2). However, our main source material will be the growing number of statements, communications, initiatives and legislative proposals about digital technology governance that have been emerging from the EU in recent months and years. These include the Commission's White Paper on Artificial Intelligence, its Data Strategy, the Digital Services Act package and the GAIA-X initiative.[2]

[1] In June 2021, Portugal will host a High-Level Ministerial Digital Assembly where it will present a "Declaration on Digital Democracy with a Purpose": a declaration of digital rights designed to establish the framework for a digital transition based on European values.

[2] Other initiatives worth mentioning at EU and global levels include the Global Partnership on AI, the WEF Global Industry Alliance, and the International Alliance for a human-centric approach to AI (IA-AI) promoted by the European Commission's Service for Foreign Policy Instruments (FPI).

1. Part 1: What we have learned?

1.1. Key technologies and determinants of their development

The three working papers in this TRIGGER work package WP4 (D4.1, D4.2 and D4.3) highlighted the breadth of the challenges faced by the EU in its efforts to shape the global governance of (and by or with) digital technologies[3]. One of the papers, D4.3, focused on a broad technology (artificial intelligence and machine learning, or AI/ML) that has countless potential domain-specific applications and that requires the balancing of a wide range of expected benefits and potential risks. The other two papers (D4.1 on open standards and open-source software, and D4.2 on distributed ledger technologies) highlighted wider considerations about the importance of technological architectures to the evolving global governance landscape.

1.1.1. Technology: artificial intelligence and machine learning (D4.3)

The field of **artificial intelligence and machine learning (AI/ML)** is perhaps the clearest example of the way in which the global governance of and by digital technologies is moving beyond technocratic best practices and becoming enmeshed in geopolitical competition. The European Commission has explicitly framed the AI/ML challenge in these terms: “The stakes could not be higher. The way we approach AI will define the world we live in. Amid fierce global competition, a solid European framework is needed” (European Commission, 2018). This backdrop shaped the analysis conducted in D4.3, which outlined key technical and governance considerations related to AI/ML and then sought to highlight the choices faced by the EU in a rapidly evolving global governance landscape. This analysis culminated in the following four key recommendations.

First, the EU should focus on concrete and domain-specific challenges and work back from there to identify the rules that are needed, rather than aiming to frame one-size-fits-all rules for all applications of a given technology. As one of the TRIGGER Scientific Committee members noted by way of example at a public TRIGGER conference held in late 2020, the stakes differ between AI/ML being deployed in different domains, e.g. in the retail sector and in law enforcement: while a mistake in the former may entail no more than an inconvenience, in the latter it could lead to wrongful imprisonment or similar serious harms.[4] To illustrate this principle

[3] In this document we use the term "by" to cover both governance "with" (where digital technology provides analytical support and decision aid) and governance "by" (where the outcome of an algorithm or a blockchain would de facto be the decision itself, such as when institutions delegate their decision-making power to machines or digital systems. See for example (Misuraca, 2020).

[4] John Zysman, speaking at the TRIGGER conference on “Governance Of and By Digital Technology”, which was organised by the International Risk Governance Center at EPFL on 18 November 2020. See https://gobdt.ch and (Zysman & Nitzberg, 2020).

of domain-specific governance, the analysis in D4.3 focused on three different uses of AI/ML: autonomous vehicles, public administration and healthcare. The insights drawn from these three domains informed a second broad recommendation, which is that **the EU should play to its strengths as an assertively normative actor by focusing on developing robust governance for those AI/ML domains that touch on fundamental rights, including privacy**. An analogy can be drawn between this "niche leadership" strategy for AI/ML and the role played by the GDPR in the governance of data protection, with assertive protection of the rights of EU citizens being used to shape global rules and behaviours. This highlights the centrality of trade-offs in the global governance of digital technologies: it is likely that prioritising a normative approach to technology governance will allow an innovation gap to persist, with other global actors, notably the US and China, continuing to be the main engines of the digital economy.[5]

The third D4.3 recommendation was that **the EU seeks to balance unity and diversity in its response(s) to AI/ML**. This touches directly on the concept of actorness, as developed and illustrated by other TRIGGER workstreams, and particularly the cohesion, authority and autonomy dimensions. In the context of a global landscape characterised by increasing geopolitical and geoeconomic competition, there is a lot to be said for the EU being able to act with one voice. However, in the context of a fast-evolving technology like machine learning, the potential benefits of regulatory experimentation across the member states should not be neglected. This need for agility and responsiveness also informed the fourth and final recommendation proposed in D4.3, which was for the EU to take steps to prevent its regulatory approach to AI/ML falling into obsolescence as AI/ML technologies and their applications evolve. Mechanisms such as "planned adaptive regulation" were suggested as a means of doing this.

1.1.2. Architecture: open standards, open-source software and blockchain technology (D4.1 and D4.2)

The two other WP4 case studies focused on considerations that relate to how open and how decentralised (or distributed) technological architectures should be. With regard to openness, von Ingersleben-Seip and Büthe note in D4.1 that **the EU has been promoting open standards and open-source software (OSS) for decades**, with both internal and external policy objectives. Internally, OSS and open standards have been seen as an engine of cross-border interoperability, which within the EU would help to develop the single market. Externally, the EU faces a trade-off in terms of the geopolitical impact of open standards and OSS. On the one hand, promoting openness involves potential adverse consequences for leading EU firms that derive significant global revenues from standard-essential patents (SEPs). On the other hand, the normative

[5] The four scenarios described below (section 2.1) provide some indications of how this trade-off could evolve, without making explicit recommendations as to how EU firms should act in order to favour their competitiveness in a world in which the US and China remain the driving forces of the digital economy.

dimension of open standards and OSS—notably the role they give to accountability, transparency and democratic participation in the policymaking process—aligns more closely with the EU's governance values than with the preferences of more authoritarian countries seeking to develop closed, government-controlled technologies. According to von Ingersleben-Seip and Büthe, this normative dimension also has potential economic benefits: insofar as the EU succeeds in promoting OSS and open standard globally, it improves the ability of EU developers to differentiate themselves when they bring open standard or OSS products to market. There is a close relationship here with the argument in D4.3 about the relationship between the normative and economic dimensions of technology governance. A strategy of niche-leadership in the governance of those AI/ML domains where normative values are particularly salient (such as healthcare or public administration) potentially boosts the global position of EU companies operating in those domains.

The analysis of **blockchain** technologies in D4.2 notes that widespread adoption of blockchain technology by organisations and the general public has yet to occur, and points to a range of governance opportunities and challenges. According to Mattila in D4.2, at a fundamental level, blockchain technology enables "a new kind of a distributed computational paradigm for rethinking how to organise human collaboration and interaction". This is a point echoed in D4.4 by Renda, who points out that the EU has a degree of affinity with the kind of decentralised, polycentric governance assumed by blockchain technology: to a certain extent, blockchain's architecture resonates with the EU's own multi-level and polycentric governance structures. Moreover, as with other emerging digital technologies, a flexible and responsive approach to the regulation of blockchain technologies in the EU could lead to innovations that bring significant societal and economic benefits. However, Mattila also cautions that widespread adoption of blockchain technologies could be disruptive at a deeper level, undermining the cohesion of global governance actors, including the EU, by freeing individuals to establish new voluntary forms of social and political organisation, along the lines of early experiments with so-called "virtual nations" such as BitNation, or with the registration of international migrants. The result may therefore need to be a hybrid or "dual-sided" form of blockchain governance, in which policymakers seek to encourage the free development of blockchain technologies while protecting the existing broad institutional system. An example here might be the European Commission's support for the International Association of Trusted Blockchain Applications (INATBA), a body that brings together developers of blockchain technologies with regulators and policymakers.[6]

[6] See also the recent suggestion by Mihail Kritikos of the EU's Scientific Foresight Unit (STOA) that blockchain may have a role to play in delivering ethical AI (Kritikos, 2020).

1.2. Key themes and priorities

There are a number of recurring themes in TRIGGER's reports on the global governance of digital technologies, and which have important consequences for the future (see part 2). One of these is the importance to the EU of **normative values** and the protection (and external projection) of fundamental rights established in the treaties. This differentiates the EU from various other global governance actors who place greater weight on freeing up innovation. This brings us to a second recurring theme: the inevitability of **trade-offs**. These need to be considered at the level of applications, because variations of a technology and their different applications in various domains entail different trade-offs. An illustration discussed in D4.3 is the trade-off between performance and explainability that often exists when AI/ML is used. An example in D4.1 is the trade-off between requiring fully open standards and maintaining the incentives for companies to invest in research and development. There are also broader governance trade-offs, including the potential trade-off mentioned above between the promotion of growth and the protection of normative values, such as fairness or privacy. It is important to note that this is not a pure trade-off: both D4.1 and D4.3 point to potential commercial advantages that the EU's normative focus can create. However, it is frequently suggested (including within the EU) that the EU's prioritisation of normative considerations in the governance of digital technologies has had the unintended effect of contributing to the relative under-development of the innovation ecosystem. And this brings us to a third important theme: the importance of **the enabling environment for technology deployment**, including industrial capacity as well as market size and structure. In the case of AI/ML, these enabling factors have played a significant role in shaping the global governance environment, with governments and regulators in the US and China seeking to allow innovation to flourish, not just as an engine of economic growth, but also as a source of geopolitical advantage. It is not yet clear how successful the EU will be with its preference—as expressed in the white paper on AI—for a rules-based approach that seeks to promote both innovation and risk-based protections. However, this is not a new challenge for the EU. It is worth recalling that in 2000, the Commission's communication on the precautionary principle stated that "decision-makers are constantly faced with the dilemma of balancing the freedom and rights of individuals, industry and organisations with the need to reduce the risk of adverse effects to the environment, human, animal or plant health" (Commission of the European Communities, 2000).

1.2.1. Actorness

The question of how much influence the EU can have in the area of global technology governance—in the context of TRIGGER, the question of how much **actorness** the EU enjoys—is an increasingly important one given the growing importance of digital technologies in the geopolitical landscape. For a detailed analysis of how each dimension of the EU's actorness has evolved in a technological domain, see the deep dive on data protection in TRIGGER's WP7. In WP4, a more concise analysis is being undertaken for each of the three case studies: AI/ML,

blockchain, and open-source software and open standards (see D4.7). The preliminary results of this exercise point to a number of interesting results, two of which we will highlight here. First, the EU is assessed to have a low level of *authority* in each of the three technologies covered in WP4, pointing to a limited capacity to enforce change directly. Second, however, the assessments suggest that the EU enjoys a much greater degree of influence, or soft power, than its formal legal authority may suggest. In each of the three case studies, the EU ranked medium-to-high on the *recognition* and *attractiveness* dimensions, suggesting that the EU is seen by third countries as an important global governance actor.

On the *credibility* dimension of actorness, the EU is assessed to be a middling performer in the three WP4 technologies. However, past weaknesses of **credibility and consistency** across digital policy as a whole are highlighted in D4.4, where Renda notes that European values have often been vaguely defined, instrumentally used and left in tension with goals such as creating European tech giants comparable to those in the US. He also points to a technological naiveté in the EU, resulting in a failure to recognise early enough key features in the recent evolution of the internet, such as the increasingly closed and proprietary nature of much of the internet, and the dominance of lightly regulated platforms. Renda sees signs of increasing coherence in the early months of the von der Leyen Commission, but cautions that a coherent EU digital policy is unlikely to lead to US-style corporate successes, precisely because numerous European values and priorities (such as fairness, sustainability, competition and data minimisation) pull in other directions. He notes that one important development in the EU's emerging data strategy is a recalibration of the bloc's commitment to global technological openness. The data strategy published in February 2020 proposes the creation of large domain-specific and cross-sectoral European "data spaces", along with the technologies and governance that will allow for the use and sharing of data, particularly by businesses. The objective is to provide the infrastructure needed to boost the EU's share of the global data economy so that it is proportionate to the EU's overall share of global economic activity.

In the next part of this report, we look ahead to the next phase of the evolution of the EU's approach to the global governance of digital technologies. We will set out the EU's long-term ambitions, as reflected in a raft of recent substantial policy proposals, and we will assess the early indications of the EU's progress in achieving these ambitions. Finally, we will draw on the work done throughout the previous reports in WP4 to provide a series of recommendations for the EU in this area.

2. Part 2: What lies ahead?

In this second part of this report, we pull together elements from part 1 and from other TRIGGER work to assess what lies ahead for the EU in the global governance of digital technologies. The aim is to present a series of principles or recommendations that should shape the EU's activities and choices in this area. We begin by briefly describing in section 2.1 the four future global governance scenarios developed by the TRIGGER project in WP5 (see D5.2). In section 2.2, we consider what a range of recent substantial EU policy proposals tells us about the EU's long-term ambitions. Section 2.3 considers the importance of trade-offs and the role of risk-based and principles-based regulation in the EU. Finally, section 2.4 draws on the work done throughout the previous reports in WP4 to provide a series of recommendations with a view to improving the ability of the EU to influence the global governance landscape for digital technologies.

2.1. Four scenarios for the EU's role in digital technology governance

Before assessing the EU's long-term ambitions in terms of the global governance of digital technology, it makes sense to consider the digital governance implications of the future scenarios that have been developed within the TRIGGER project. The scenarios presented in WP5 describe four possible futures for the global governance landscape by 2050, with a particular focus on the role of the EU. The scenarios are designed to provide a frame for thinking about long-term trajectories and goals, so that we can assess where the EU is (or should be) heading. In the context of digital technology, the implications of the four scenarios differ dramatically[7].

- In the first scenario, "Gaia", global governance has transformed in 2050 into an effective and stable constellation of actor-network powers operating under a planetary systems approach to decision-making and action. Digital technology governance has become a fluid balancing of demands within a network of actors. The EU is a relatively weak actor, but it has a strong legacy and influence. Regarding AI/ML, the ethical guidelines for AI that emerged from the earlier years of large-scale system deployments have been hardcoded into the fundamental source code from which actor-network specific AI systems are forged. These guidelines contain specific fail-safes and boundary conditions that limit 'worst-case' scenario behaviours from AI, and include specific human oversight mechanisms that are mandatory. In other words, in the Gaia scenario, the EU's strong focus on principles and values is embedded into software. So, while Gaia may not support geopolitical ambitions of technological sovereignty, by ensuring that fundamental principles are respected when laws are put in codes and algorithms to reflect the values

[7] For an exploration of EU public sector innovation in a data-driven society, see the scenarios developed by the Joint Research Centre (Misuraca et al., 2020).

and goals of the community, Gaia supports the EU's overarching goal of a high-technology society that is respectful of privacy, ethics and other fundamental rights.

- In the second scenario, "Duplomacy", global governance has become fragmented. The geopolitical landscape is divided into four power blocks with little cooperation among them. Despite the collapse of traditional global governance institutions, the EU is an internally unified, coherent political actor, earning legitimacy from its citizenry by focusing on increasing the quality and accessibility of services for all its constituents. In this context, the EU makes extensive use of digital technology such as AI/ML and has established strong governance policies that address accuracy of outcome, data-based biases, explainability of the outcome, actor accountability, transparency, and human oversight. Although personal data and privacy are not prioritised within the bloc, they are tightly secured from external forces via advanced encryption. The achievement of Duplomacy would mean that the EU has increased its sovereignty. It is a strong power, both in terms of technology and regulation. However, this has been possible thanks to the fragmentation of the world into blocks that are isolated from each other and defend their territory from external influence. There is little global cooperation, and so little scope for innovative and collaborative global developments in digital technology and its governance.
- In the third scenario, "Reunited Nations", the world has transformed (like in Gaia), and the EU has a strong influence (like in Duplomacy). Global institutions have been re-designed and re-oriented in ways that explicitly build on EU priorities and values: modern, nimble and fostering ecological justice, human and non-human rights, and the peaceful cohabitation of the planet. Speaking with a more unified voice, the EU is able to exert a stronger influence on global governance by bolstering existing institutions and their efficacy. Digital technologies play a pivotal role in this world, and as Renda notes in D4.5, in a world like this, the EU is well-positioned to seek global backing for its approach to technology, particularly in terms of ensuring protection for fundamental rights. In Reunited Nations, technology plays an important role in governance. Open-source AI/ML technologies are widely deployed and strictly regulated with regards to design protocols, data analysis techniques, security and privacy standards, and accountability for outcomes. Blockchain has been deployed for incentivising citizen action and verifying various data transactions.

  The pursuit of the Reunited Nations scenario would be desirable in terms of the achievement of the EU's ambition regarding digital technology and governance. The scenario is very optimistic regarding the ability of the EU to become a global leader, in part because its principled stance on technology governance appeals to many countries undergoing rapid development. Under this scenario, the EU is able to use its value-based approach to foster collaboration and cooperation with a large coalition of nations, which can have many side benefits (trade, influence in global governance, etc.)

- In the fourth scenario, “World Wide Gaps”, the world is fragmented (as in Duplomacy), but the EU’s influence is weak (like in Gaia). Global wealth has been severely concentrated in the hands of very few state powers, individuals, and private organisations. This has fractured the efficacy of global governance mechanisms and institutions, weakened the power of democratic states, and reinforced divisions between social classes. The EU’s strength has been undermined, as its member states (themselves highly unequal in prosperity and influence) struggle to find common ground for policy and action. Under World Wide Gaps, there is a growing difference in technological development between different territories, with highly localised solutions paired to competing private standards, a highly fragmented internet, and a deepening digital divide. There is little oversight of AI/ML, and few options to question the increasing use of “black-box” algorithmic decision-making. The use of digital technology for mass surveillance and manipulation becomes the norm.

  In this scenario, the EU is too weak to protect its values-based approach to technology governance, let alone project it as a model to be followed globally. This scenario is highly undesirable for the EU. Its vision of a world in which technology runs rampant and private interests determine societal outcomes is anathema to the values and traditions on which the EU is founded. Already, aspects of current EU technology policy are motivated by preventing the realisation of a World Wide Gaps scenario, such as the aim of the Digital Markets Act to limit the power of “gatekeeper” internet platforms.

2.2. EU ambitions and initiatives

There are three key ambitions that characterise the EU’s approach to the governance of digital technologies. Resolving the potential for tensions between them is likely to be a central pillar of the EU’s activities in the years ahead. The first two ambitions are the promotion of (competitive) economic activity and the protection of citizens’ fundamental rights. The third, and more recent, ambition is the idea of digital or technological sovereignty, which is a key focus of recent proposals from the European Commission. All three of these ambitions should currently be understood in the wider context of an unsettled geopolitical and geoeconomic landscape, in which patterns of rivalry and cooperation are in flux and in which digital technologies are playing an increasingly important role as a source of economic growth and a marker of international status.

The challenge of governing digital technologies in a way that balances different goals is not a new one for the EU. In WP7, the deep dive on data protection shows how in the 1980s and 1990s, the EU learned how to complement its original economic priorities with the increased focus on fundamental rights that emerged as the EU evolved into an increasingly political entity. The ambition of technological sovereignty did not exist as such during the period when the EU was developing its governance approach to data protection. Nevertheless, the key legislative milestones (the 1995 Directive and the 2016 GDPR) can be interpreted in these terms, as a

process that harmonised the rules being applied within the EU and then projected them extraterritorially to be followed by third-countries that wanted to maintain economic ties with the EU. However, while the EU enjoys what we might term regulatory sovereignty in the data protection area, this has not led to the EU becoming a centre of gravity to rival the US in terms of digital economic activity. In other words, the EU may increasingly set the terms on which cross-border data flows can take place, but the companies that have commercialised these data flows are not predominantly from the EU. (One argument is that the EU's data protection rules actively inhibit the development of the "domestic" technology sector by inhibiting the range of data that can be exploited in the development of new AI/ML technologies and applications.)

These three ambitions have been reflected in a number of substantial policy proposals from the European Commission over the last two years, which collectively represent an important statement of intent as to the direction of digital technology governance in the EU. These should also be seen in the context of the December 2020 "Berlin Declaration on Digital Society and Value-based Digital Government", in which all EU member states signed up to a set of seven key principles (European Commission, 2020f). The next step for the EU will be to spell out in increasing detail what this direction of travel will require in operational terms in order to be effective. The key policy documents are as follows:

- **White Paper on AI** (European Commission, 2020d)**.** The Commission's white paper subtitled "A European approach to excellence and trust" establishes a clear dual ambition. On the one hand, AI/ML should support innovation and growth through the creation of an "ecosystem of excellence"; on the other hand, normative checks and balances should be put in place through the creation of an "ecosystem of trust" to determine what is allowed and not allowed. The ecosystem of excellence requires action at multiple levels, including working with member states, boosting support for the research and innovation community, and partnering with the private sector. Concerning the development of the trust ecosystem, the Commission indicates a preference for a risk-based approach that would focus regulation on high-risk activities. The excellence and trust goals align quite clearly with the first two ambitions discussed above: economic growth and fundamental rights. The white paper's focus on sovereignty is weaker, but it does note at one point that "harnessing the capacity of the EU to invest in next-generation technologies and infrastructures, as well as in digital competences like data literacy, will increase Europe's technological sovereignty in key enabling technologies and infrastructures for the data economy". Further provisions relating to AI regulation are included in the resolution on a "framework of ethical aspects of artificial intelligence, robotics and related technologies" adopted by the European Parliament on 20 October 2020 (European Parliament, 2020).

- **A European Strategy for Data** (European Commission, 2020c)**.** The Communication of the Commission on the European strategy for data published in February 2020 also combines elements of the three ambitions. There is an economic imperative at its root, a recognition that the EU risks being left behind if the US and China maintain their innovation lead as the data economy matures. Therefore, the strategy aims, by 2030, for Europe to have a share of the data economy that matches its economic weight, and it also envisages a complementary industrial strategy that would foster the development of a new ecosystem of data-driven companies, products and services. For example, the data strategy notes that the pooling of data across the EU would enable the development of the AI/ML sector. In terms of fundamental rights, the strategy states that the EU rules and values will apply across the new "single European data space". International data flows will be encouraged, but will be subject to an "assertive" enforcement of European values. This aligns with the technological sovereignty ambition of being able to set rules and insist that everyone operating in a rapidly growing European data space complies with them.

- **The Digital Services Act and Digital Markets Act** (European Commission, 2020a, 2020b)**.** This package of two new proposed regulations combines the aims of boosting economic activity and protecting fundamental rights. The economic objective of the Digital Services Act is reflected in the fact that the proposal is based in Article 114 of the Treaty on the Functioning of the European Union, which concerns the smooth functioning of the internal market. In this sense, the primary aim of the proposal is to "ensure harmonised conditions for innovative cross-border services to develop in the Union" and to "establish a level playing field to foster innovation, growth, and competitiveness". At the same time, the protection of fundamental rights plays a key role. The backdrop for the Commission's proposal is the transformation of the digital ecosystem since the e-Commerce Directive was adopted in 2000, with the explosion of new digital services, notably including online platforms, such as social media and marketplaces. These new services have led to new "challenges and risks", and the proposed regulation seeks to ensure that the EU's rules are fit for purpose in terms of "online safety and the protection of fundamental rights".

  At the same time as publishing its digital services proposals, the Commission also published its draft of an accompanying regulation on digital markets (European Commission, 2020b). This aims to ensure that the market for digital services is contested and fair, with a particular focus on what are described as "gatekeeper" platforms, which "enjoy an entrenched and durable position" and therefore often wield significant control over the smaller businesses that rely on their services.

- **GAIA-X.** The GAIA-X initiative is a joint project initiated by France and Germany and now includes more than 120 partners. It is a federated cloud infrastructure, the aim being to level the competitive playing field by giving the same data access to small and large players. As Renda notes in D4.5, the creation of a pan-European cloud infrastructure reflects the EU's ambition of technological sovereignty, in particular by developing the scale necessary to compete with US tech giants. Germany's Federal Ministry for Economic Affairs puts GAIA-X firmly in the context of EU sovereignty: "We must safeguard our strategic capacity for action in order to be able to operate digitally in the long term on a free and self-determined basis. For this, we must also maintain digital sovereignty in the realm of data" (Federal Ministry for Economic Affairs and Energy, 2019). GAIA-X also highlights the EU's economic ambitions, anticipating a new wave of digital transformation in which a combination of emerging technologies and innovative governance leads to growth being driven by regulators that succeed in fostering vibrant, competitive and interoperable ecosystems rather than by seeking to promote dominant giants in concentrated markets. The fundamental rights ambition is less pronounced in discussions of GAIA-X thus far, but the assumption is that (as with the single data space discussed above) its cloud specifications would be compliant with EU rules and values on questions such as data protection, trust and security.

2.3. Governance and trade-offs

One of the most important challenges facing the EU with regard to its ambitions for digital technology will be deciding on how to resolve trade-offs that are likely to arise between them. The process of evaluating and resolving trade-offs is a pivotal part of governance, as it can highlight the costs as well as the benefits that different policies or ambitions may entail, and it can have a significant impact on the ultimate trajectory towards achieving the various long-term ambitions. As noted above, the EU's approach to data protection provides an example here: the introduction (and global projection) of strong values-driven data protection rules has contributed to the EU as a "super-regulator", but it has also arguably contributed to the EU's relative weakness in terms of innovation and the size of the digital economy.

The importance of having transparent processes for resolving trade-offs between ambitions is that it requires clear decisions about which costs (or risks) are acceptable and which are not. For example, in D4.3, the authors have suggested that the EU should follow a "niche leadership" strategy in the AI/ML field. This would allow the EU to carve out a position of strength in those domains where core EU values such as privacy, trust and fairness are highly salient, but there is an acknowledgement that prioritising values in this way will likely mean ceding a lot of digital economic activity to more commercially assertive players.

Two important approaches to governance in the EU are principles-based governance and risk-based governance. In general terms, **principles-based regulation** means relying on high-level, broadly stated rules to set the standards that have to be complied with, rather than detailed prescriptive rules (Hopper et al., 2007). It is not easy to find pure examples of this approach in the EU. The GDPR is motivated by fundamental principles, but it translates these into quite specific prescriptive rules. By contrast, the principles for trustworthiness recommended by the High-Level Expert Group on AI are less prescriptive, but they are also non-binding.

Risk-based regulation "achieves public policy objectives by targeting activities that pose the highest risk to the public well-being, and in turn lowers burdens for a variety of lower-risk sectors and firms." (World Bank Group, 2017) The risk-based approach has become popular in many countries, in part because of the promise that economic activity will be protected if low-risk activities are actively targeted with lower compliance requirements. However, this approach involves many challenges, beginning with the definition of what is at risk. Risk-based regulation requires a thorough evaluation of benefits and risks, and should result in a regulatory system that prioritises the proportionality of regulation to the risk profile of the activity being regulated.

As discussed in the previous section, the White Paper on AI adopts a risk-based approach, and the same applies to the forthcoming AI regulation expected in April 2021. While this is welcome—and is also in line with much EU regulatory practice, including the Better Regulation Toolbox (European Commission, 2017)—it is far from obvious how AI/ML-related risks would be characterised and measured in a sufficiently granular manner to allow regulation. The White Paper states: "A given AI application should generally be considered high-risk in light of what is at stake, considering whether both the sector and the intended use involve significant risks, in particular from the viewpoint of protection of safety, consumer rights and fundamental rights".[8]

2.4. Recommendations

This report concludes with nine recommendations for the EU related to the governance of and by digital technology. We believe that prioritising these recommendations could help make progress on a number of important concerns, thereby increasing the EU's actorness and its ability to influence the evolving global governance landscape for digital technologies.

1. Prioritise regulation of algorithmic decision-making

The principle that technology should be at the service of humans, and not vice versa, is at the core of the EU's values and traditions. This human-centric approach to technology has particular relevance in relation to artificial intelligence and machine learning (AI/ML). In D4.3, the authors discussed AI/ML, focusing on the particular concerns that arise when the outcome of an ML

[8] See also D4.3, as well as Section 4 of The Governance of Decision-Making Algorithms report (IRGC, 2018).

system is directly and immediately used to make and implement decisions, without human intervention or control. High-profile and contentious examples include applications in autonomous driving or those that use facial recognition technologies. But caution is needed, even when algorithmic decision-making is used in more seemingly innocuous contexts. For example, the Commission's White Paper on AI suggests that the use of AI/ML in a hospital's appointment scheduling system is unlikely to warrant regulatory intervention (European Commission, 2020d). One could counter that there are numerous ways in which such a system could lead to harmful or inequitable outcomes, and that such outcomes might be more likely to persist in the absence of human oversight. The EU should therefore ensure that any algorithmic decision-making that concerns critical matters for consumers and citizens and occurs without appropriate human oversight is treated for regulatory purposes as a high-risk application[9]. However, industrial automation governed by AI would not fall under the category of high-risk applications. The appropriate type and mode of human oversight may differ depending on an evidence-based assessment of the risks involved. In January 2021, the European Parliament adopted a resolution calling for guidelines to ensure that AI does not replace either human decision-making or human contact. It also calls for a ban on "highly intrusive social scoring applications" by public authorities, and expresses concerns over "deepfakes" (European Parliament, 2021).

2. Be clearer about how risk-based and principles-based regulation are used

As discussed in section 2.3, there are important differences between risk-based and principles-based approaches to regulation. There is a role for both in the EU's governance of digital technologies, but it is important to develop both in a clear, nuanced, consistent and implementable way. The EU has emerged as a global regulatory leader in its emphasis on fundamental individual rights as a keystone of technology governance. This principles-based ethos is a powerful one. Among other things, it helps to identify where ethical boundaries should be drawn (see recommendation six below). But it is important to see the elaboration and operationalisation of such governance principles as an ongoing task, in order to prevent ambiguity (technical or philosophical) from reducing the principles' real-world traction. Philosophically, there must be clarity and consensus on what the principles mean; principles like fairness or equality can mean different things to different people. Technically, it must be possible to operationalise the principles: developers must be able to understand and implement them in code.

Risk-based approaches to regulation begin with an assessment of the risks: who might be harmed, in what way, and with what severity? Then a range of regulatory responses is drawn up, including details of how rules are enforced and who is accountable for AI harms. Risk assessment should be conducted at the domain-specific level rather than across whole technologies (see

[9] See list of high-risk sectors and uses or purposes, in appendix to Framework of ethical aspects of artificial intelligence, robotics and related technologies (European Parliament, 2020).

recommendation four below). The process must also involve more than a technical assessment of potential harms and exposures. It should consider the wider societal and political context, including the views (opinions, perceptions, concerns, expectations) of those who use or are otherwise affected by technologies, and the risk assessment should feed into an evaluation process where legitimate societal decisions can be taken about whether or how much of the risks under assessment are deemed acceptable (IRGC, 2017). A serious complication here is that for evolving risks like those from digital technologies, ex-ante and one-off risk assessments are not sufficient. Monitoring of impact (ex-post) and ongoing changes are needed, which will call for adaptive governance mechanisms that co-evolve with the risk. The EU is increasingly incorporating a risk-based element into its governance of digital technologies, notably in the recent White Paper on AI, but arguably the White Paper presents a restricted binary distinction between high-risk and low-risk applications of AI/ML, which does not match the complexity and variety of the risk landscape for a potentially ubiquitous technology like AI/ML. In the US, an executive order on trustworthy AI, issued in December 2020, also refers to risk, requiring agencies to use AI "where the benefits of doing so significantly outweigh the risks, and the risks can be assessed and managed" (White House, 2020). Important follow-up is expected from the Biden Administration (Engler, 2021).

3. Consider applying the precautionary principle to AI/ML

As formulated in the EU, the precautionary principle states that: (i) action should be taken where there are reasonable grounds for concerns, on the basis of preliminary objective scientific assessment, about (ii) potential dangerous effects that may be inconsistent with the high level of protection chosen for the community, but where (iii) "scientific evaluation does not allow the risk to be determined with sufficient certainty" (Commission, 2000). The principle has been applied mainly to the management of risks to the environment and human health. It may be worth explicitly expanding the scope of the precautionary principle to cover a wider range of potential risks posed by digital technologies, such as potential irreversible damage to fundamental rights, for example. Another argument for considering the precautionary principle here is that the speed with which new digital technologies can propagate across societies can outstrip the pace at which a robust evidence base can be developed as to the impacts of those technologies. Application of the precautionary principle can be contentious, however, for example, if it is interpreted as requiring harm-avoidance measures unless there is "full scientific certainty" about a technology's impacts, and when it is seen as hindering innovation.[10] Nuanced expressions of the precautionary principle require deliberation as to what action should be taken. Sandin (1999) states simply that the principle requires "some kind of action" to be taken. The Commission (2000) states more pointedly

[10] Cf the Rio Declaration, Principle 15: "In order to protect the environment, the precautionary approach shall be widely applied by States according to their capabilities. Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation."(United Nations, 1992)

that measures based on the precautionary principle should comply with a range of criteria, including being "proportional to the chosen level of protection".[11] This returns us to the question of risk evaluation mentioned in the previous recommendation: in order to decide what kind of precautions are warranted, it is necessary to have a (political) evaluation of the seriousness of the risks that a given technology might cause. It is worth noting that the proposed expansion of the precautionary principle to cover digital technologies is in line with the "Ethics Guidelines for Trustworthy AI" produced by the EU's High-Level Expert Group on AI (2019a), and recommended under certain conditions by the group in its subsequent "Policy and Investment Recommendations" (AI HLEG, 2019).

4. Focus on domain-specific regulation

This is one of the key recommendations that emerged from the analysis of AI/ML in the D4.3 report. It should shape the EU's approach to the governance of digital technologies more generally, after consideration of important value principles, and in order to operationalise principles and general guidelines into concrete policy action. In other words, the primary focus of policymakers should not be on technologies per se, but on their application, i.e. sectors and use or purposes, because this is where risks arise. An additional point is that within these domains, policy should not focus only on those aspects of a technology that may need to be restricted or regulated in some way. Where appropriate, policymakers should also advocate for the increasing use of digital technologies that can mitigate domain-specific risks, such as various forms of privacy-preserving technologies, for example (see recommendation five). Indeed, the more empowering or enabling technologies become, the more likely they are to change the nature and scope of the risks that they may bring, both in terms of: a) undesirable outcomes, i.e. possible damages or losses, and b) missed desirable outcomes, i.e. potential benefits and advantages. Therefore, both undesirable and missed desirable outcomes of technologies should be considered in a balanced risk assessment.

While the domain-specific level should be the primary focus of governance measures, this should not be allowed to prevent a more holistic view of the technology governance landscape. A siloed approach that *only* considers the risks and responses in individual domains may miss important interdependencies and wider systemic vulnerabilities. One way of achieving this balance might be to consider both "horizontal" principle-based regulation "vertical" risk-based regulation in specific domains, looking at both sector of application and particular uses/purposes.

[11] The Commission lists five other criteria. Measures based on the precautionary principle should also be: non-discriminatory, consistent, based on an examination of costs and benefits, subject to review, and capable of assigning responsibility for producing scientific evidence that would allow for a more comprehensive risk assessment.

5. Invest in the development and implementation of technology for privacy and trustworthiness

With a view to balancing the twin ambitions of economic growth and fundamental rights, the EU should invest in and incentivise the development and use of technologies that help to protect fundamental rights "by design". This means paying greater attention to "governance by digital technology" alongside the more familiar "governance of digital technology", in recognition of the fact that technology can help to solve some important governance challenges. Two key examples here relate to areas where the EU has already positioned itself as a leader. The first of these is privacy and data protection, where the EU enjoys the status of super-regulator with significant extra-territorial reach. However, concerns have been raised about the inhibiting effect that strong data protection rules can have on the development of data-driven industries. The EU is cognisant of these concerns, and, as noted above, its data strategy explicitly aims to create greater freedom to tap into the commercial possibilities offered by the huge quantities of data that are generated across the EU. Within this strategy, the EU should prioritise the development and deployment of enabling technologies, such as various confidential computing techniques that offer a potential "risk-superior" solution on the trade-off between privacy and growth.

A second area where the EU could catalyse the development of technology-led growth is in relation to trustworthiness. As Renda notes in D4.5, the EU has made progress towards using the principle of trustworthiness. Building trust in digital technologies relies on various factors, including technical robustness and safety; privacy and data governance; human agency and oversight; diversity, non-discrimination and fairness; societal and environmental well-being; transparency (traceability and explainability); accountability (impact assessment and redressing). The EU should seek to incentivise those technological solutions that contribute to achieving one or more of these requirements for trustworthiness. This potentially includes the use of solutions that would embed legal rules (and the values those rules express) in technical specifications that could be mandated across the EU—this thinking informs the GAIA-X initiative discussed above. However, a distinction should also be maintained between "ethics by design", which embed by default the ethical rules in the technology, and "pro-ethical design" that more broadly contributes to design environments that can facilitate ethical choices, actions or processes. Both approaches are liberal, but ethics by design may be mildly paternalistic, insofar as it privileges the facilitation of the right kind of choices, actions, process, or interactions on behalf of the agents involved. Whereas pro-ethical design does not have to be paternalistic, insofar as it privileges the facilitation of reflection by the agents involved in their choices, actions, or process (Floridi, 2014).

6. Define ethical red lines

One consequence of a clearer and more consistent use of principles-based and risk-based approaches to the governance of digital technologies should be greater clarity over where the EU's red lines lie. A transparent and legitimate process is needed to assess (and review

periodically) whether there any applications of any digital technologies that should be ruled out regardless of the potential benefits they may offer, because the risks they pose are too great to countenance, or because of their incompatibility with the EU's fundamental values. For example, the German Data Ethics Commission has recommended that at a threshold of "untenable potential for harm", AI/ML applications should be subject to a complete or partial ban (2020). An example given of such an application is a lethal autonomous weapons system ("killer robot") in which killings are decided on by an algorithm. The Commission's White Paper on AI does not specify any applications that might be subject to a ban, although it does promise a "broad European debate" on the use of remote biometric identification (such as facial recognition) in public places, because this raises "specific risks for fundamental rights" (European Commission, 2020d).

There is also a broader question here about the alignment of the EU's approach to digital technology governance with its other normative priorities. Of particular relevance here is the EU's increasing focus on climate change and achieving carbon neutrality. Digital technologies may play a huge role in policy responses to climate change, but they can also be highly energy-intensive. Optimising the energy footprint of digital technologies may require changes in the prevailing cloud-based paradigm towards new architectures. For example, edge computing optimises cloud computing systems by performing data processing at the edge of the network, near the source of data (for example, performing more computation at the level of the sensors capturing the data). Fog computing implements a decentralised computing infrastructure in which data, computing, storage and applications are distributed in the most logical, efficient place between the data source and the cloud. Other areas where it is possible to reduce energy consumption include reducing the energy consumed in the production of digital technology goods, and reducing their obsolescence (Craglia et al., 2018). There is a trade-off between the short and long terms to be considered here: causing some carbon emissions in the short term in order to deliver a technology ecosystem that will lower the global carbon footprint.

In this respect, it is worth noting that the EU data strategy includes a €2 billion "High Impact Project" for data processing architectures, tools and infrastructure designed to foster a gradual rebalancing between centralised data infrastructure in the cloud and highly distributed and smart data processing at the edge (European Commission, 2020c).

7. Clarify the scope, rationale and goals of technological sovereignty

Sovereignty is a contested political concept, and there are additional complications to consider in the context of a multi-level governance system like the EU's. In this context, greater clarity is needed as to the intention and concrete implications of the EU's goal of digital or technological sovereignty. There are fundamental questions here about how the EU intends to engage with the

rest of the world (see recommendation nine below). The backdrop for the Commission's increasing focus on sovereignty and related concepts (such as "open strategic autonomy") is provided by the period of geopolitical uncertainty and change that the world is currently undergoing. Technological sovereignty can be understood in this context as the objective of ensuring that the EU retains the value of its digital resources and is able to make and enforce decisions about the use of digital technologies across its territories. But what does this mean in practice? How should the EU seek to achieve its sovereignty aims: by setting its own rules and requiring everyone to comply with them, or by agreeing to shared rules? Should the EU's aims be achieved through working only with states, or by promoting soft law approaches that bring in private sector actors and standards bodies? It is worth noting that one of the lessons of the Brexit process over recent years is that in a deeply interconnected world, the relationship between sovereignty and power or effectiveness is not straightforward. Prioritising sovereignty is not without potential downsides, and so the EU should spell out what it sees as the costs as well as the benefits of this approach. It should also explain in greater detail how sovereignty in the technological domain might interact with developments in other major domains of global interdependency, including climate, trade and competition policy.

8. Balance public and private forms of governance

The EU should weigh the relative pros and cons of public and private forms of governance with regard to maximising its effectiveness at shaping the global governance landscape. The EU has shown with the GDPR that it has the heft required to project rules globally, but it would be unwise to generalise too swiftly from the data protection case to digital technologies more generally and conclude that flagship regulations are the most effective way of proceeding. There may be instances where the EU would enjoy more leverage through seeking to influence sectoral standards, guidelines and codes of conduct, ex-ante conformity assessments or self-regulation more generally. However, compliance and enforcement are a particular challenge with such forms of governance. Platform governance is likely to be a key test-bed for mixed public-private approaches to digital technology governance.

9. Develop a strategy for working with other key global governance actors

Building on recommendation number seven, the EU should clarify how it intends to work with other key actors. The most important of these are the US and China, given the clear leadership role these countries play in the development and deployment of digital technologies. Acknowledging the complexity of the EU's relationships with these countries is a crucial starting point if the EU is to find a consistent and durable way of acting on its goal of increased sovereignty and autonomy. As the authors of D4.3 noted, the EU is much closer in terms of its political, cultural and societal values to the US than to China. This can be seen in the recent Commission call for a "joint technology agenda" with the US (and potentially with a wider group of "like-minded

democracies" (European Commission, 2020e)). However, it will need to be clarified whether or how such a joint agenda might constrain the EU's technological sovereignty. And the EU may also need to prepare for US questions about whether a joint agenda in this area is undermined by the EU's decision to deepen its economic ties with China without first aligning with the US. One question here may be whether there are "lowest common denominator" governance principles that the EU could agree with other global actors. Like a series of concentric circles, there may be differing levels of consensus that could be achieved with different groupings: only a very thin agreement might be possible between all three of the US, China and the EU, whereas a much greater level of overlap is likely to be possible between the EU and US.

3. Concluding remarks

The actorness/effectiveness framework used by TRIGGER provides a powerful way of analysing the position and performance of the EU in any policy domain. Arguably, it is ultimately effectiveness that matters: the ability of the EU to achieve its goals. Actorness is a means to that end, and in the digital domain, we can see that for each of the three EU ambitions discussed in section 2.2 above, different dimensions of actorness move into prominence.

Of the three ambitions, the EU's actorness is strongest with respect to the protection of citizens' fundamental rights. To a significant extent, this position rests on the cumulative success the EU has had throughout the decades-long evolution of its governance of data protection, culminating in the hugely influential GDPR. During this process, the EU has developed across every dimension of actorness, but four stand out. Of the internal dimensions, the EU is particularly strong on cohesion and authority. On the external dimensions, it is unrivalled for recognition and also enjoys high levels of attractiveness.

The EU's success at influencing the global governance of data protection perhaps offers a model for how it can help to shape the global "rules of the road" in other areas of digital policy. The dual-nature of the attractiveness dimension is important in this. The strength of the EU in protecting fundamental rights does not rest solely on normative factors, though these play an important role. The EU has also been willing to leverage its huge market power to force external actors to play by its rules, through extraterritoriality provisions, adequacy agreements and other similar measures. The use of economic conditionality is likely to be a powerful source of influence in relation to rule-setting in many other areas.

However, while this approach can shape the rules that apply across the EU, it has little traction in terms of driving innovation and data-driven growth. In D4.3, the authors framed this as a clear trade-off between the ambition of protecting fundamental rights and the ambition of driving up levels of growth and innovation in the EU. The argument there was that in seeking to balance rights and growth, the EU is likely to prosper as an innovation hub mainly for a number of digital technology "niches" where that impinge particularly clearly on fundamental rights and values. Obviously, the EU's ambitions stretch far beyond such a niche economic role. As we have seen, the data strategy sets a 10-year target of closing the gap between the EU's data-economy performance and its overall economic weight. Renda is correct in D4.5 when he frames the ambition as one of becoming a digital-economy "third power" alongside the US and China.

Boosting economic activity in this way is a challenge of a different order compared to setting the rules with a legal instrument like the GDPR. It means influencing the decisions of individuals and companies about what activities to undertake, and where to do so. It is likely to require a step-change in industrial policy, aimed at creating an enabling environment for innovating businesses

across Europe. This is the goal of the EU's data strategy and of initiatives like GAIA-X. And it is possible that the emerging wave of new digital technologies is particularly well-suited to the needs of a hybrid polity like the EU. For example, federated computing infrastructures may minimise the relevance of the fragmentation that is inevitable across 27 member states, making it easier to drive growth with an innovation ecosystem comprised of many diverse actors rather than dominated by a small number of giants. This is the wager that the EU, in effect, is currently making.

In terms of the relation of the growth ambition to the dimensions of actorness, recognition and attractiveness stand out. These are external dimensions in the actorness framework, but arguably they also exert an important internal constraint here. Unless and until the EU is recognised as an attractive base in which to launch and build data-driven businesses, then aggregate levels of economic activity are likely to suffer due to innovators and investors choosing other locations. There is a potential tension here with the fundamental rights ambition, and the EU has work to do to convince innovators and investors that the huge focus on (and success of) its efforts to build a new data-related regulatory architecture won't inhibit support for innovation.

Internal dimensions of actorness also come into play here. There is weak cohesion across the EU about how far the bloc should go in promoting economic growth, particularly if it is perceived as being at the expensive of the European social model. (One way of countering this argument may be to draw on the idea of technological sovereignty, and suggesting that protection of the European social model means encouraging a wave of EU innovation and growth as a counterweight against the growing societal influence of tech giants from outside the EU.) Weak cohesion over policies towards growth—including significant reluctance to harmonise in key areas such as fiscal policy and industrial policy—also leads to significant weaknesses on the other internal dimensions of actorness. In the absence of greater cohesion, the EU is unlikely to be granted increasing authority or autonomy over economic policy.

The ambition for EU technological sovereignty is perhaps best understood in terms of the "opportunity/necessity to act" dimension of actorness. The world is rapidly evolving, and that the EU risks being left behind both normatively and economically if it allows digital innovation and the data economy to be carved up between the US and China. In this sense, there is a geopolitical or geoeconomic necessity to act, in order to prevent the EU's relative decline. And as Renda notes in D4.5, this *necessity* to act may now be coinciding with a window in which there is a "once-in-a-generation" *opportunity* to act, because the latest phase of the digital transition can still be shaped. The ambition of technological sovereignty is closely related to the other two ambitions. It means being able to decide and enforce rules protecting rights and values. It also means developing the digital-economy weight necessary to compete with the world's other major powers across a wide spectrum of digital technologies. But as noted above, in the absence of greater cohesion across the EU on key aspects of economic policy, the EU may not enjoy much authority

or autonomy to directly drive growth. Perhaps one way of thinking about the role of the EU here is not in terms of actorness and external influence, but as an internal catalyst. If technological sovereignty is to be realised, it will require deeper consensus than currently exists about how the ambitions of fundamental rights and economic growth (or precaution and innovation, to phrase it another way) should be balanced in the decades ahead. This touches on fundamental questions of political economy. If the EU institutions can help find alignment on such questions—between the member states, of course, but also with the private sector, the wider innovation ecosystem and civil society—it would be an important contribution to building the foundations for future EU actorness and effectiveness.

Bibliography

AI HLEG. (2019). *Ethics Guidelines for Trustworthy Artificial Intelligence*. European Commission. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419

Commission of the European Communities. (2000). *Communication from the Commission on the precautionary principle*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52000DC0001&from=EN

Craglia, M., Annoni, A., Benczúr, P., Bertoldi, P., Delipetrev, B., De Prato, G., Feijóo, C., Macias, E., Gómez, E., Iglesias, M., Junklewitz, H., Lopez-Cobo, M., Martens, B., Nascimento, S., Nativi, S., Polvora, A., Sanchez, I., Tolan, S., Tuomi, I., & Vesnić Alujević, L. (2018). *Artificial Intelligence: A European Perspective*. https://doi.org/10.2760/11251

Engler, A. (2021, 21 January). 6 developments that will define AI governance in 2021. *Brookings*. https://www.brookings.edu/research/6-developments-that-will-define-ai-governance-in-2021/

European Commission. (2017). *Better regulation toolbox*. European Commission - European Commission. https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox/better-regulation-toolbox_en

European Commission. (2018). *Artificial Intelligence for Europe*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN

European Commission. (2020a). *Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*. https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-parliament-and-council-single-market-digital-services-digital

European Commission. (2020b). *Proposal for a regulation of the European Parliament and of the council on contestable and fair markets in the digital sector (Digital Markets Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0842

European Commission. (2020c). *A European strategy for data*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN

European Commission. (2020d). *White Paper on Artificial Intelligence: Public consultation towards a European approach for excellence and trust*. https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence

European Commission. (2020e). *Joint Communication to the European Parliament, the European Council and the Council—A new EU-US agenda for global change*. European Commission. https://ec.europa.eu/info/sites/info/files/joint-communication-eu-us-agenda_en.pdf

European Commission. (2020f, 8 December). *Berlin Declaration on Digital Society and Value-based Digital Government*. Shaping Europe's Digital Future - European Commission. https://ec.europa.eu/digital-single-market/en/news/berlin-declaration-digital-society-and-value-based-digital-government

European Parliament. (2020, 20 October). *Framework of ethical aspects of artificial intelligence, robotics and related technologies*. https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html

European Parliament. (2021, 20 January). *Guidelines for military and non-military use of Artificial Intelligence*. https://www.europarl.europa.eu/news/en/press-room/20210114IPR95627/guidelines-for-military-and-non-military-use-of-artificial-intelligence

Federal Ministry for Economic Affairs and Energy. (2019). *Project GAIA-X – A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem*. 56.

Floridi, L. (2014). *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford University Press UK.

German Data Ethics Commission. (2020). *Opinion of the Data Ethics Commission*. Bundesministerium der Justiz und für Verbraucherschutz. https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN_lang.html;jsessionid=41204A6F1D8568642B04D085A0AFB000.1_cid334?nn=11678512

Hopper, M., Band, C., & Llp, H. S. (2007). Making a success of Principles-based regulation. *Law and Financial Markets Review*, 16.

IRGC. (2017). *Introduction to the IRGC Risk Governance Framework* (REP_WORK). EPFL. https://doi.org/10.5075/epfl-irgc-233739

IRGC. (2018). *Workshop Report: The Governance of Decision-Making Algorithms* (REP_WORK). EPFL IRGC. https://doi.org/10.5075/epfl-irgc-261264

Kritikos, M. (2020, December). What if blockchain could ensure ethical AI? *Panel for the Future of Science and Technology*. https://www.europarl.europa.eu/stoa/en/document/EPRS_ATA(2020)656334

Misuraca, G. (2020). Rethinking democracy in the "pandemic society" a journey in search of the governance with, of and by AI. *CEUR Workshop Proc.*, 1–13.

Misuraca, G., Barcevičius, E., & Codagnone, C. (2020). *Exploring digital government transformation in the EU: Understanding public sector innovation in a data-driven society.* Joint Research Centre (European Commission). http://op.europa.eu/en/publication-detail/-/publication/86598559-fd56-11ea-b44f-01aa75ed71a1/language-en

Portuguese Presidency of the Council of the European Union. (2021). *Priorities | EU2021PT*. EU 2021. https://www.2021portugal.eu/en/programme/priorities/

Sandin, P. (1999). Dimensions of the Precautionary Principle. *Human and Ecological Risk Assessment: An International Journal*, *5*(5), 889–907. https://doi.org/10.1080/10807039991289185

United Nations. (1992). *Rio Declaration on Environment and Development*. https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_CONF.151_26_Vol.I_Declaration.pdfvVaw3Lnivykcjc30OI_LqSPGVA

White House. (2020). *Executive Order on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-promoting-use-trustworthy-artificial-intelligence-federal-government/

World Bank Group. (2017, January). *Risk-Based Regulation | World Bank Group*. Olc.Worldbank.Org. https://olc.worldbank.org/content/risk-based-regulation

Zysman, J., & Nitzberg, M. (2020). *Governing AI: Understanding the Limits, Possibilities, and Risks of AI in an Era of Intelligent Tools and Systems*. Wilson Center. https://www.wilsoncenter.org/publication/governing-ai-understanding-limits-possibilities-and-risks-ai-era-intelligent-tools-and

INSTITUTION EURASIAN INSTITUTE
OF INTERNATIONAL RELATIONS

trigger

Trends In Global Governance and Europe's Role

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