Transnational digital governance and its impact on artificial intelligence

Section 3: Developing an AI Governance Regulatory Ecosystem

Mark Dempsey, Executive MPA Graduate & Technology Policy Researcher, Hertie School, Berlin, Germany

Keegan McBride, Postdoctoral Researcher, Hertie School, Berlin, Germany and Mohammed Bin Rashid School of Government, Dubai, UAE

Meeri Haataja, CEO & Co-Founder, Saidot, Helsinki, Finland

Joanna Bryson, Professor of Ethics and Technology, Centre for Digital Governance, Hertie School, Berlin, Germany

Abstract: The rapid pace of technological advancement and innovation has put existing governance and regulatory mechanisms to the test. There is a clear need for new and innovative regulatory mechanisms that enable governments to successfully manage the integration of digital technologies into our societies, and to ensure that such integration occurs in a sustainable, beneficial, and just manner. Artificial Intelligence (AI) stands out as one of the most debated such innovations. What exactly is it, how should it be built and deployed, how can it be used, and how should it be regulated? Yet across the period of this debate, AI is becoming widely utilized and addressed within existing, evolving, and bespoke regulatory contexts. The present chapter explores the extant governance of AI, and in particular what is arguably the most successful AI regulatory approach to date, that of the European Union. We explore core definitional concepts, shared understandings, values, and approaches currently in play. We argue that not only are the Union's regulations locally effective, but, due to the so-called 'Brussels effect', regulatory initiatives within the European Union also have a much broader global impact. As such, they warrant close consideration.

Introduction

The continual process of societal digitalization has led to a dynamic and almost amorphous regulatory environment. Compare the regulation of digital technologies to that of say, pharmaceutical drugs, consumer-grade food products, or investment instruments, and it becomes clear that the degree of regulatory understanding and policy precision differs widely, despite the fact that digital technologies can have just as much impact on human cognitive and neurological capacities, health, and development as our medicine, food, and finances. One of the most important digital-technology concepts currently at play within this dynamic is that of Artificial Intelligence (AI). Having a clearly defined regulatory environment for AI would be helpful for developing not only widely shared understandings of the technology, but more urgently to ultimately enable governments to protect their citizens' interests and coordinate at a global scale to address issues that cannot be contained by national borders.

One leading model of transnational coordination is the European Union (EU), a political and economic union of nations with harmonised law only specifically where member nations agree by treaty to so harmonise. Founded in 1993, the zone of the EU's partially shared currency (the euro), has become persistently one of the world's three largest economies. The region is also taking increasing leadership roles in global issues such as sustainability, health, and climate.

AI regulation has become a priority for the EU's executive branch of government, the European Commission ('the Commission'). In her recent first speech before the European Parliament, the new president of the Commission, Ursula von der Leyen, committed to adopting "a coordinated European approach on the human and ethical implications of artificial intelligence." (Von der Leyen, March 2020, pg. 13)

In today's digitalized world, transnational dependencies are increasingly common, and therefore transnational regulatory and governance frameworks are needed that take these dependencies into account. The way that the European Union (EU) is handling digital regulation generally, and AI in particular, is of great interest because they are charting new territory in this space that can provide valuable learnings to governments globally. Because the EU is a trading bloc of independently functioning and historically warring nations who now 'harmonize' their legislation to create unified market policies, its mechanisms for building consensus and coordination across a multiplicity of cultural and governance structures is particularly likely to be both useful and even instructive. Further, in addition to the trans-national but within-jurisdiction nature of EU legislation, academics have recently increasingly examined extra-territorial impacts of EU law, as what has become known as 'the Brussels Effect' (Bradford, 2021). This and similar effects for other regions is an important further focus of this chapter.

With all of this in mind, this chapter charts the most salient attempts to date in providing global and transnational governance frameworks for AI worldwide, but with an emphasis on existing EU regulatory acts and proposals. Such acts include the General Data Protection Act which aims at digital privacy widely, including for AI. Proposals include the Digital Services Act (DSA) focussing on impacts and remedies for familiar platform AI such as Websearch and social media, and the EU Commission's more recent Artificial Intelligence Act (AIA)¹, which focuses on identifying and regulating potentially hazardous applications of the technology. We start first with a brief definition of terms as they will be used in this chapter and follow with an overview of existing transnational AI governance efforts. The ensuing sections delve deeper into the EU regulatory process, its development over time and its culmination in the "Brussels Effect" of EU law as mentioned above and which occurs upon the fulfilment of several conditions. The closing sections of the chapter assess two of the major EU regulatory proposals governing AI: the Digital Services Act (DSA) and the AI Act (AIA).

Defining AI & Context

Definitions of AI abound, varying in their technical precision, legal utility, and prescriptive versus descriptive quality. AI is all around us (Bryson & Wyatt, 1997) and like other systems, it can often be made out to be more complicated than need be. Unfortunately, such convolution in particularly regulatory contexts may often be deliberate aiming to advance an agenda or bypass potential scrutiny. In addition to this, AI remains a contested concept also given its universality as a general-purpose technology (Bryson & Brundage 2016). Thus, to date, there has been difficulty when it comes to reaching consensus on a single definition of AI. This dispersed state of definitional affairs increases confusion and has negative implications for the regulation and governance of AI.

It is important to examine the interests and ambitions driving certain definitions of AI with a critical lens. For example, the Organization for Economic Co-operation and Development (OECD) has a *trade and economic progress mandate*; this is reflected in their definition, which it published with its OECD

¹ The European Commission published the "Proposal for a Regulation of the European Parliament and of the Council - Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts" on April 21, 2021

principles on AI². According to the OECD, an “Artificial Intelligence (AI) System is a machine-based system that can, for a given set of human defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments” (OECD, 2021, p. 7).

Such a definition can be contrasted to that offered by the EU’s proposed AIA which states that:

“...‘artificial intelligence system’ (AI system) means software that is developed with one or more techniques and approaches listed in Annex 1 (of the AIA)³ and can, for a given set of human-defined objectives, generate outputs, such as content, predictions, recommendations, or decisions influencing the environments they interact with” (AIA, 2021, p. 2)⁴.

These definitions are broad, but for the purpose of this chapter we will use an even broader and more succinct definition for AI: “AI is any artifact that extends our own capacities to perceive and act” (Bryson, 2019). Although it is an unusual definition, it might, as Bryson notes, “...also give us a firmer grip on the sorts of changes AI brings to our society, by allowing us to examine a longer history of technological interventions” (Bryson, 2019). Further, it does so while capturing the essential core of the previously listed definitions – producing or altering action in a context via an artefact – while avoiding the hazard of trying to list (even in a relatively easy-to-update appendix) all the means by which this might be achieved.

An overview of existing transnational AI governance efforts

Transnational AI governance is becoming increasingly important, and research on the topic has begun to rapidly proliferate, especially research focusing on the regulation and global coordination of such regulation for technological advances (Erdélyi et al., 2018; Deeks, 2020; Crotoft et al., 2021; Beaumier et al., 2020). However, many scholars fail to sufficiently acknowledge or discuss pre-existing AI regulatory policy, which has evolved over several decades. Research and deployment of AI has, so far, been primarily ‘up-regulated’ with very significant government and other capital investments (Miguel and Casado, 2016; Technology Council Committee on Technology, 2016; Brundage and Bryson, 2016; cf. Bryson 2019).

In the context of the above, there are two important points to note:

- No one is talking about introducing regulation to AI. AI already exists and has always existed in a regulatory framework (Brundage and Bryson, 2017; O’Reilly, 2017). What is being discussed is whether that framework needs optimizing.
- Regulation has so far mostly been entirely constructive, with governments providing vast resources to companies and universities developing AI. Even where regulation constrains, informed and well-designed constraints can lead to more sustainable and even faster growth.

² Agreed in May 2019 by 42 states and adopted by the G20 in 2019; See Artificial Intelligence OECD Principles on AI, available at <https://www.oecd.org/going-digital/ai/principles/>

³ Annex 1 includes the following techniques and approaches:

“(a) Machine learning approaches including supervised, unsupervised and reinforcement learning, using a wider variety of methods including deep learning.

(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines (symbolic) reasoning and expert systems;

(c) Statistical approaches, Bayesian estimation, search and optimization methods.” (AIA Annex 1, 2021, p.1)

⁴ Charlotte Stix provides a detailed overview and analysis of the EU Commission’s AIA proposal in this manual under *Section 9: International Politics and AI Governance*

In this regard, it is possible to draw comparisons to the finance sector. Finance has always been regulated, but, as the global financial crisis (GFC) of 2007-2009 demonstrated, regulations must be overhauled and optimized. We are at similar cross-roads with AI. As the technologist Benedict Evans argues: “[Information] Tech has gone from being just one of many industries, to being systemically important to society.” (Evans, 2020) If something is ‘systemically important to society’, it must be governed and regulated. Indeed, day to day life is becoming increasingly intertwined with AI. The welfare of society and citizens may be influenced by decisions that are becoming increasingly made by algorithms. Such changes have led to extensive research (e.g., AlgorithmWatch, 2020; EU Fundamental Rights Agency, 2020) and a further drive for ‘downwards regulation’ – constraint – not least where privacy, surveillance, bias, and discrimination are concerned.

The lack of any formal regulatory structure to address AI concerns on a transnational level, and to legally hold corporations (including ‘platforms’) and governments to account, has led to the rapid emergence of international governance and ethics fora; political fora, and standards developing efforts. Between 2016 and 2019, for example, more than 80 AI ethics documents – including codes, principles, frameworks, and policy strategies – have been produced by corporations, governments, and NGOs (Schiff et al., 2019). Perhaps the OECD Principles on AI come closest to a global consensus with 42 signatory states⁵. The core five OECD principles were soon subsequently adopted as the G20 AI Principles⁶, bringing the total number of signatory states to 50. The OECD Principles, combined with the United Nations Sustainable Development Goals, are now core frameworks for all efforts by the Global Partnership on AI, another recent transnational AI ‘initiative’.

The Global Partnership on AI (GPAI), just mentioned, is another example of a recent high-profile initiative in AI governance. Launched in June 2020, it consisted at initiation of 15 partners⁷. In December 2020, four additional nations were admitted, and UNESCO became a member of the partnership as an observer. The GPAI is intended to be the preeminent global forum where working groups of chosen AI experts and practitioners meet to discuss and inform policy in a multidisciplinary approach. The present goal is for the GPAI to ‘bridge the gap between theory and practice on AI’. (GPAI, April 2021). Interestingly GPAI is not explicitly portrayed as a governance mechanism, in fact its terms of reference prohibit ‘normative’ outcomes. Nevertheless, in establishing a partnership developing shared governmental capacities in the cooperative deployment of AI interventions, it has clear impacts and consequences for AI transnational governance. Coinciding with the development of different transnational organizations, studies are also beginning to become increasingly available that map the content of existing principles and guidelines for AI regulation around the globe. Such studies aim to understand where a global agreement on AI guidelines is emerging or indeed has emerged (Jobin et al. 2019, Lorenz, 2020). Such research suggests growing global convergence around five ethical principles – transparency, justice and fairness, non-maleficence, responsibility, and privacy and defence of the human individual (Jobin et al., 2019; Bryson 2017).

These principles correspond well to principles retained within the OECD and G20 approaches to AI, to which most wealthy nations are signatories, including: all members of the EU, the USA, and China. Nevertheless, some argue that substantive divergences exist in how these principles should be

⁵ See Artificial intelligence > OECD Principles on AI, available at <https://www.oecd.org/going-digital/ai/principles/>

⁶ See G20 AI Principles, available at <https://www.g20-insights.org/wp-content/uploads/2019/07/G20-Japan-AI-Principles.pdf>

⁷ See GPAI: Global Partnership on Artificial Intelligence, available at <https://gpai.ai/>

interpreted, applied, and moreover question the usefulness of guidelines and principles. Principles tend to act a means of formalizing non-binding guidelines for national governments to abide by and they remain attractive to “condense complex ethical considerations or requirements into formats accessible to a significant portion of society, including both the developers and users of AI technology” (Stix, 2021, p. 2) as well as by providing a useful starting point from which to develop more formal standards and regulation (Whittlestone et al. 2019). Principles are sometimes seen as too high level, difficult to practically implement, and particularly prone to manipulation – especially by industry (Rességuier et al., 2020). Nevertheless, the OECD has a good history of first expending effort gaining consensus around principles, and then seeing them implemented as law by member nations. This process of legislation is being followed now by several institutions, notably the EU.

EU regulatory process

That the EU has led the way with proposals to legislate AI and digital technology more widely should not necessarily be a surprise. The development of the Digital Single Market has long been recognized as a priority by the European Commission’s Digital Single Market Strategy (DSM)⁸ — such strategy has formed an important piece of President von der Leyen’s Commission agenda for Europe 2019–2024⁹. Digital regulation in the EU, including efforts to regulate AI, are first and foremost about the need to ensure the efficient functioning of the Single Market. But this functioning must be based on the four freedoms: of goods, services, capital, and labour. Additionally, the “European Approach” to digital governance aims to ensure that development is done in a way that is consistent with the EU values of human dignity, freedom, democracy, equality, rule of law and human rights.¹⁰

In the past, the EU has been accused of regulatory activism and, most notably by former President Obama, as being protectionist, but there is little evidence to support this claim. In fact, recent judgements when analysed suggest the opposite (Bradford, 2020, pg. 104). Rather, the EU is simply a tough regulator whether against foreign or domestic firms. EU citizens and NGOs have demanded more protective regulations and have been vocal in demanding more stringent consumer, environmental, and health protections than their counterparts in other parts of the world. It is also well known that EU citizens are particularly distrustful of the conduct of dominant companies in the digital realm and are more concerned about the integrity of their personal data which in turn has led to regimes such as the GDPR (Pfeiffer et al., 2021)¹¹.

The EU’s tendency to harmonize¹² standards upwards has also been facilitated by changes to EU Treaties that have enabled regulations and directives to be adopted with a qualified majority¹³ of the Council as opposed to unanimity. The move towards qualified majority voting (QMV) goes back to the

⁸ See Questions and Answers on the Digital Single Market Strategy, available at https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_4920

⁹ See ‘A Union that strives for more. My agenda for Europe’, available at https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

¹⁰ See: https://europa.eu/european-union/about-eu/eu-in-brief_en

¹¹ Whilst much of this is derived from Europe’s own history, this includes the imposition of strong antitrust regulation on Germany by the allies following WWII, and led by the USA (Wu, 2018).

¹² The harmonization of standards is one of the drivers towards ensuring the integrity of the Single Market. For example, inconsistent product standards can hinder cross-border trade. The Single Market guarantees the free movement of goods and ensure seamless trade between EU member states.

¹³ QMV requires the support of 55% of member states representing the minimum of 65% of the EU’s population.

adoption of the Single European Act (SEA)¹⁴, which came into force in 1987 and paved the way to completing the Single Market by 1993, and the four freedoms as mentioned previously. The ability to proceed with legislation, even in the absence of consensus, established the foundation for significant rulemaking in the aftermath of the SEA. Had member states insisted on unanimity as the default decision-making rule, it is doubtful that the ambitious regulatory agendas that have been undertaken by the EU over the last 30 odd years would have emerged (Bradford, 2020).

Such ambitious regulatory agendas have driven the development of extensive scholarship, which aims to understand the true regulatory reach of European institutions, and the emergence of the EU as a or even the principal shaper of global standards across a wide range of areas (Bradford, 2012; Schwartz, 2019; Scott, 2016; Bradford, 2020). Often called “soft power with a hard edge” (Goldthau et al. 2015), the EU makes up for its lack of hard power through its use of policy and regulatory tools. Compliance with EU policy is motivated by access to its enormous market. Often, as in the case of the general data privacy regulation (GDPR), the same regulatory acts not only set out measures to protect individuals within that market, but also to smooth and harmonise access to the full market, with the ultimate goal of a net positive increase in both commerce and other aspects of well-being.

The ‘Brussels Effect’, a term coined by the EU law scholar Anu Bradford, refers to the EU’s unilateral ability to regulate the global marketplace. This can occur ‘*de facto*’ when global corporations respond to EU regulations by adjusting their global conduct to EU rules. No regulatory response by foreign governments is needed; corporations have the business incentive to extend the EU regulations to govern their worldwide production or operations simply because of the EU’s own economic strength when taken as a unitary actor, combined with the utility of simplicity in maintaining a relatively unified product offering world-wide.

The ‘Brussels Effect’ is considered ‘*de jure*’ when the governments of third countries (those outside the EU) adopt EU-style regulations after global corporations have adapted their global conduct rules to conform to EU rules. In this case, companies often have the incentive to lobby their governments for higher standards in their home jurisdictions. This ensures that they are not at a disadvantage when competing domestically against companies that do not export to the EU and that, therefore, have no incentive to conform their conduct or production to potentially costly EU regulations (Bradford, 2020).

Bradford (2020) asserts that for the ‘Brussels Effect’ to occur, five conditions need to be cumulatively met. However, follow-up research has found that in practice it can occur in the absence of some criteria being fulfilled (Preusse et al., 2020). Bradford’s five conditions for the ‘Brussels Effect’ are: sufficient market size, regulatory capacity, stringent standards, inelastic targets, and non-divisibility.

Market Size: The EU Single market is the world’s largest single market area in which goods can move freely. It is also a place where the Commission’s goal of high safety standards and the protection of the environment is maintained by stringent regulations. It accounts for 450 million consumers and 22.5 million small and medium-sized enterprises (SMEs)¹⁵. As Bradford notes “*Large market size is, indeed, a pre-condition for unilateral regulatory globalization. Yet the jurisdiction must also possess*

¹⁴ See Single European Act (SEA), available at <https://www.europarl.europa.eu/about-parliament/en/in-the-past/the-parliament-and-the-treaties/single-european-act>

¹⁵ See *Internal Market, Industry, Entrepreneurship and SMEs*, available at https://ec.europa.eu/growth/singlemarket_en#:~:text=The%20EU%20Single%20Market%20accounts,the%20protection%20of%20the%20environment.

sufficient regulatory capacity to exercise global regulatory authority".¹⁶ The EU at least is largely able to regulate its own markets in terms of the products its citizens and residents are exposed to.

Regulatory Capacity: The EU has institutional structures in place that can adopt and enforce regulations effectively¹⁷ and which themselves reflect the preferences of its key stakeholders, EU citizens. But what sets the EU apart is the depth of its regulatory expertise and resources with which it can enforce its rules and thereby exert its authority over market participants – within or outside of its jurisdiction. In the case of non-compliance, the EU imposes sanctions. Only jurisdictions with the capacity to impose significant financial penalties on others (as the EU often has) or exclude non-complying firms from their market can force regulatory adjustment (Bradford, 2014).

Inelastic targets: These targets do not refer to the traditional usage of inelasticity in economics (sensitivities of demand when variables such as price change), but rather to the products or producers that are regulated by the EU. In the case of the Brussels Effect, the location of the consumer within the EU, as opposed to the location of the manufacturer, determines the application of EU regulation to the targeted product. Union geography is largely inelastic but can alter with Union membership.

Stringent Regulations: Studies (Gausch et al; Elliott et al., as cited in Bradford, 2020) show that wealthier states are more likely to have higher domestic demand for stringent regulations. Beyond the EU's use of a stringent regulatory agenda as a tool for promoting further integration, there are also two crucial factors that differentiate the EU from other states and regions in its demand for tough regulations (Bradford, 2020):

- Europe's greater belief in government rather than markets as the means to generate fair and efficient outcomes (ideology), (Pew Research, 2018).
- An environment in Europe where higher relative importance is given to public regulation over private litigation and a lower threshold for intervention by regulators in case of uncertainty (process).

Note that this "greater" belief in government is relative to the apparent trade-offs made in some other large regulatory regions, but not necessarily all. No markets are entirely free of regulation, nor is any government fully controlling its economy, what varies is the extent of reliance on these two strategies. Also note that differences in beliefs concerning such trade-offs may be justified by real regional variation in governing capacity.

Non-divisibility: This refers to the practice of standardizing – in this case when a company standardizes its production or business practices across jurisdictions. Bradford (2020) differentiates between '*legal non-divisibility*', when legal requirements and remedies drive uniform standards (for example in the case of a merger where rules of the jurisdiction with toughest competition laws prevail), and '*technical non-divisibility*' which refers to the difficulty of separating the firm's production or services across multiple markets for technological reasons. Either form increases regulatory power, but the EU's special concerns and legislative efforts of course most affect the former.

¹⁶ Bradford, A. 2020. The Brussels Effect: How the European Union rules the world. Oxford University Press, pp 24

¹⁷ EU regulatory capacity has been developed since the adoption of the Single European Act (SEA) which launched the ambitious agenda to complete the Single Market by 1992. To implement this goal, EU member states vested the EU institutions with powers to formulate and enforce regulations.

The EU Commission's Presently Proposed Regulations: The Digital Services Act (DSA) and the AI Act (AIA)

The Digital Services Act (DSA)¹⁸ and the Commission's proposal to regulate AI systems ('the AIA')¹⁹ were published on 15 December 2020 and 21 April 2021, respectively. At the time of writing, both proposals have spawned global conversations, for example on how to regulate the large technology platforms (which are ostensibly the focus of the DSA) and the use of digital automation by public sector authorities (arguably one of the main targets of the AIA). The reaction to both these proposals is not unlike the wave of debate about the nature of data privacy that followed the enactment of the GDPR, and which continues today. This section provides a perspective on both proposals but starts by regarding privacy and its status within European digital legislation.

The significance of privacy as a fundamental right

It is important to understand the significance of privacy in Europe as a core component of the EU's digital legislation. The philosophy behind the EU's fundamental rights approach to privacy is to foster self-determination of individuals by granting them enhanced control over their personal data (Lynsky, 2020). This philosophy can be traced back to The European Convention of Human Rights (ECHR)²⁰, a treaty document which guarantees a fundamental right to privacy, drafted not by the EU, but by the older and significantly larger Council of Europe. All EU member states are among the 47 signatories to the ECHR, making all Europe beneficiary of its privacy rules. However, it was not until 2009 that the Lisbon Treaty gave legal force to the Charter, despite it having been "solemnly proclaimed" by the European Parliament, Council of Ministers, and the European Commission (but not the Member States) at Nice in December 2000 (Anderson et al., 2011). At the time it lacked the binding force of law, but as Anderson notes:

"The Convention members had decided to proceed on the basis that the Charter should be drafted 'as if' it might be legally binding," and further "its 54 Articles — which are for the most part replicated in the Charter as finally adopted in 2007 — were thus drafted with an eye to the possibility of judicial enforcement." (Anderson et al., 2011, p. 10).

Similarly, the GDPR also furthers the goal of protecting EU citizens, their data, and their privacy. Privacy scholar, Paul Schwartz (2019) put the impact of the GDPR as follows:

"Proof of the influence of the GDPR and EU data protection law...goes beyond the hefty sums spent by U.S. companies to comply with them. The EU has taken an essential role in shaping how the world thinks about data privacy. Even corporate America draws on EU-Centric language in discussing data privacy" (Schwartz, 2019, p. 3)"

The EU frames the extraterritorial reach of the GDPR and justifies the measures it has taken to enforce compliance with the law, because they are necessary to ensure the continued protection of

¹⁸ Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) See: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en>

¹⁹ Proposal for a Regulation on a European approach for Artificial Intelligence. See: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

²⁰ See European Convention on Human Rights, available at https://www.echr.coe.int/documents/convention_eng.pdf

fundamental rights of EU residents when their data are processed beyond EU borders. This reasoning is echoed in the DSA and the AIA.

The Digital Services Act (DSA) and the AIA

The DSA and the AIA proposals represent a seismic shift in how the EU regards digital policy, moving from voluntary codes to legally binding regulatory structures to ensure more accountability, transparency, and responsible behaviour from market participants. Over the last 20 years, there has not been a meaningful attempt to ‘regulate the Internet’²¹. This is now changing.

The DSA builds on the existing e-Commerce Directive²², which was adopted in 2000, and was the first attempt by the EU to set up a framework to remove obstacles to cross border online services in the Internal Market. The e-Commerce Directive is acknowledged as being the first piece of EU regulation that set clear limits on liability for digital platforms – meaning that they were not held responsible for illegal material uploaded to their sites, but rather only responsible for bringing down illegal material when informed. In other words, without this legal safe harbour, the Internet would likely not have grown to what it is today, as this would have restricted the publishing of user-generated content (Echikson, 2017).

The e-Commerce Directive has also had important consequences in allowing the digital culture in Europe to evolve. It enabled digital firms in one EU member state to do business in another without any restrictions and it stipulated, importantly, that when they do so, it is the ‘country-of-origin rules’ that apply for most purposes. This remains the case with the DSA. The ‘country-of-origin’ principle is a key principle that was laid out in the e-Commerce Directive whereby providers of online services are subject to the law of the Member State in which they are established and exempts online intermediaries from liability for the content they manage, if they fulfil certain conditions²³ (European Parliamentary Research Service, 2020)

Further to building upon the e-Commerce Directive, the DSA, and its twin piece of legislation which deals with market competition rules, the Digital Markets Act (DMA), are directly applicable as regulations, as is the intention with the AIA, which is also a proposal for a regulation. In that regard, all these documents will have binding legal force in each EU member state. In contrast, a directive outlines certain outcomes that must be achieved but each member state is free to decide how the directive is transposed into national law. The legal designation of regulations further emphasizes the significance and importance of these new rules for the Commission and the EU institutions and their wider digital regulatory agendas.

²¹ See ‘This is why the government should never control the internet’, available at <https://www.washingtonpost.com/posteverything/wp/2014/07/14/this-is-why-the-government-should-never-control-the-internet/>

²² See Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, available at <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031>

²³ An example is the Safe Harbour Privacy Principles which were developed between 1998 and 2000 and were designed to prevent private organizations within the European Union or United States which store customer data from accidentally disclosing or losing personal information. The seven principles from 2000 are: notice, choice, onward transfer, security, data integrity, access, and enforcement (See Wikipedia: https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles)

The AIA follows the Commission's '*White Paper on Artificial Intelligence: A European approach to excellence and trust*'²⁴ which was published in February 2020 as a follow up to its *European Approach to Artificial Intelligence* strategy document from April 2018²⁵. The White Paper can be seen as an effort to understand via a wide consultative process whether there was a need firstly, to update regulatory checks on AI systems across sectors as they currently exist, and, if so, how they might best fit into a formal, binding legislative framework. The White Paper proposed several ideas and structures which informed the AIA²⁶. At the centre of the White Paper, and as is consistent with the OECD and earlier Principles, and the framings of the DSA, DMA, and the GDPR, are concepts of safety, fairness, transparency, and data protection.

A closer look at the Digital Services Act

The liability exemptions in the e-Commerce Directive have been maintained in the DSA, where the firms that provide 'transmission' (Digital Service Act, December 2020, p. 45) of information in a communication network ('mere conduit', 'caching') and storage of information ('hosting' but without looking at what is being hosted) escape liability. It therefore behoves the platform to prove in individual cases that it had no 'actual knowledge' of illegal content in its pages or that it has acted 'without undue delay' to remove such content or block access to it.

The Commission also proposes a new set of obligations for firms of different sizes, with firms below a certain threshold considered micro-, small- and medium-sized firms and thus exempt from new transparency and disclosure obligations. Firms are defined as "very large online platforms" as those "...online platforms which provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million" (Digital Service Act, December 2020, p. 60) – equivalent to 10% of the Union's population.

The transparency obligations (Articles 26–33) for very large platforms sets this proposal apart from the GDPR. It may have been drafted with competition considerations in mind given that the GDPR reinforced, and in some cases strengthened, the market positions of large firms like Google, while smaller firms lost market share due to the disproportionate burden of costs to revenue experienced in meeting the regulation's demands (Peukert et al., 2020). The thresholds suggest that the Commission has reviewed some of the unforeseen impacts of the GDPR, though such remediation might be better met with true proportionality rather than thresholds. Nevertheless, in the draft versions at least, the 10% threshold as mentioned above applies to all firms that supply services to EU businesses and consumers whether they are based in Europe or not. In this aspect, the DSA will apply on an extraterritorial basis as is the case with the GDPR.

As regards content moderation, the DSA introduces several specific obligations which include, for example, the requirement that companies already carrying out content moderation must submit annual reports to authorities outlining their approach. There are further provisions regarding the takedown of illegal content with obligations to report why it was taken down (or wasn't) with EU

²⁴ See White Paper on Artificial Intelligence - A European approach to excellence and trust, available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

²⁵ See Artificial Intelligence for Europe, available at <https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF>

²⁶ The White Paper was just one of several exercises that informed the AIA; any formal proposal from the Commission must be preceded by a formal impact assessment. To the end the Commission published a study supporting the impact assessment of the AIA: <https://digital-strategy.ec.europa.eu/en/library/study-supporting-impact-assessment-ai-regulation>

citizens having the right to challenge and platforms required to respond within a specified time frame. The rights of appeal are explicitly outlined. These new protections for consumers have been welcomed by rights groups and consumer associations (Access Now, 2020; AlgorithmWatch, 2020.)

Further obligations to strengthen consumer protection in the DSA concern advertising transparency; Article 24 obliges platforms to provide the following information: “(a) that the information displayed is an advertisement; (b) the natural or legal person on whose behalf the advertisement is displayed; (c) meaningful information about the main parameters used to determine the recipient to whom the advertisement is displayed”. (Digital Services Act, December 2020, p. 58). But these have been widely criticized as not going far enough but rather regarded as simply reinforcing the status-quo since many platforms “already allow users to see some basic information about ads and ad targeting and have created ad databases”. (Blankert & Jaursch, 2021).

European Digital Rights, an influential pan-European body, whilst complimentary of the EU’s attempts to provide further transparency around advertising, suggests that in this area the DSA “...completely fails to address the problems inherent in the toxic ad tech business. Without any limitations to the micro-targeted online manipulation through ad tech (and with a strong ePrivacy Regulation nowhere to be seen), the constant surveillance of people across the internet for the purpose of online advertising remains the norm.” (EDRI, December 2020)

A contentious section of the DSA proposal concerns the need to report on risks. For ‘significant systemic risks’, platforms are required to identify, present a plan to mitigate, and then to report back on the efficacy of their risk mitigation measures. Reporting of anything that raises risks of dissemination of illegal content is not controversial; rather it will be determining the risk of “any negative effects for the exercise of fundamental rights to respect for private and family life, freedom of expression and information, prohibition of discrimination and rights of the child” (Digital Services Act, December 2020, p. 61) that leaves plenty of room for dispute. On a positive note, this obligation and clause as it has been worded clearly shows the intent by the Commission to protect all rights as per the European Charter for Fundamental Rights (ECFR). What this means in practice, and what it implies for firms remains an active debate at the time of publication in advance of the proposal being passed into law. The DSA is not expected to be implemented till 2023.

Access to data, auditing, and enforceability

The emphasis on transparency is a very welcome part of the approach to the DSA by the Commission; for example, Article 31 on ‘data access and scrutiny’ marks a significant and major progressive step in allowing authorities to scrutinize how platforms target, moderate, and recommend content or services to their users. Under this Article, vetted researchers will be able to apply to access platform data for the purpose of “conducting research that contributes to the identification and understanding of systemic risks,” (Digital Services Act, December 2020, p. 63) including potential negative effects on fundamental rights or civic discourse.

For data access to work effectively, the US-based Brookings Institute believes that the Commission:

“... could set up a centralized process that enables secure data access to researchers without this capacity. The United States has effectively implemented this through systems like the Census Bureau’s Statistical Research Data Centers and the Coleridge Initiative’s Administrative Data Research Facility.” (Engler, January 2021)

The empowering of newly created independent bodies – Digital Services Coordinators (DSCs) – at the Member State level to carry out onsite inspections is a positive step, but DSCs cannot be effective unless they are fully resourced and willing and able to use the new powers that this act proposes. The same goes for the use of independent auditors who will undertake mandatory audits of the large platforms and that have “proven expertise in the area of risk management,” as well as “technical competence” (Digital Services Act preamble, December 2020, p. 34) to audit algorithms. These requirements may indicate the need for new higher education degree programmes to train enough appropriate staff for AI developing organisations, their auditors, and regulators alike. It may though be sufficient to expand existing systems-engineering courses in computer science departments, but there may be a need to also to create specialist programming courses specifically for auditing and certification rather than full-scale development. Software development like any creative act displays wide degrees in variation of talent, but it should not be necessary to compete for the top creative talent to find those well-suited to assessing the claims being generated by the DSA.

Producing adequate competence in these areas is an achievable goal. The period of transition both before the DSA becomes law but also the formative years of the legislation will be crucial and lobbying efforts to dilute the effect of new laws will be significant. It is important that the DSCs are established and stabilized quickly so commerce is not negatively impacted with too much uncertainty, and also that there is a constructive dialogue between the DSCs and market participants as a means of allowing experiments to be tried without poor first attempts getting established as permanent precedent. Moreover, regulatory capture by agencies and individuals with vested interests is also a threat and one that can hopefully be addressed through the same measures and standards of transparency being applied within these tools of governance as they are intended to apply without.

A brief assessment of the EU AIA²⁷

The EU deserves credit for being the first among international political organizations or states to propose a regulatory framework for updating AI systems: an immense task given the cross-cutting nature of such systems. Furthermore, the EU’s insistence on basing such a framework on European values and fundamental rights can hopefully again set a high global bar. In terms of international law, it would be a very significant and positive global development if its final-form regulatory framework were to achieve for the concepts of AI transparency and trustworthiness what GDPR has achieved for the concept of privacy.

In 2018, the Commission published a strategy for AI entitled “Artificial Intelligence for Europe”²⁸. It is a broad and wide-ranging document laying out the EU approach towards AI over a series of steps which includes allaying public fears, updating the EU safety framework to address liability gaps and legal uncertainty, as well as announcing investments into training schemes and grants to AI-based start-ups. An overarching message was that the ‘EU will not leave people behind’ and language deployed throughout mirrored that from the GDPR – privacy, trust, values, and ethics. The plan proposed close EU cooperation across four key areas: increasing investment, making more data available, fostering talent, and ensuring trust.

The Commission’s *The White Paper: On Artificial Intelligence — A European approach to excellence and trust* (“the White Paper”) went a step further when it proposed policy options to “enable a

²⁷ Much of this section is taken from a working paper by two of the co-authors of this chapter; see Haataja & Bryson, “Reflections on the EU’s AIA and how we could make it even better”, 2021, *in preparation*.

²⁸ See Artificial Intelligence for Europe, available at <https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF>

trustworthy and secure development of AI in Europe in full respect of the values and rights of EU citizens,” (EU AI White Paper, February 2020, p.3). The extensive stakeholder consultation that followed the White Paper showed that a large number of stakeholders “were largely supportive of regulatory intervention to address the challenges and concerns raised by the increasing use of AI” (Explanatory Memorandum, *Proposal for a Regulation on a European approach for Artificial Intelligence*, April 2021, p.1) and together with explicit requests from the European Parliament and the European Council led to the formal regulatory proposal.

The regulatory proposal was announced as part of a broader package, *A European Approach to Excellence in AI*, targeting to strengthen and foster Europe’s potential to compete globally. Therefore, while our focus here is on the regulatory proposal itself, it is useful to understand the larger context and the accompanying coordinated plan on AI (2021 review) which details the strategy for fighting for Europe’s competitiveness in AI. “Through the Digital Europe and Horizon Europe programmes, the Commission plans to invest €1 billion per year in AI. It will mobilise additional investments from the private sector and the Member States in order to reach an annual investment volume of €20 billion over the course of this decade. And the newly adopted Recovery and Resilience Facility makes €134 billion available for digital. This will be a game-changer, allowing Europe to amplify its ambitions and become a global leader in developing cutting-edge, trustworthy AI.”²⁹ This corresponds to roughly €65 billion investment volume annually by 2025³⁰.

The regulatory proposal is part of a continuum of actions that started in 2017 with the European Parliament’s Resolution on Civil Law Rules on Robotics and AI³¹ and entailed several other key milestones³² prior to the proposal at hand. It is addressed to AI use cases that pose a high risk to people’s health, safety, or fundamental rights. All other uses of AI are explicitly *not* addressed in the new Act, with the understanding that they are already regulated by standard existing frameworks. The new regulations would apply to all providers and deployers placing on the market or putting into service high-risk AI systems in the European Union, regardless of the origin of the providing entity. In this way, the proposal seeks to level the playing field for EU and non-EU players and has mechanisms to influence far beyond its immediate scope (extra-territorial reach).

We now turn to discuss a few of the concepts of the AIA which appear to us to be solid and actionable. These concepts may well therefore also be the most important elements for other regions beyond the EU to consider for their own AI policy.

Clear and actionable framework for AI risk levels. The proposal suggests a risk-based approach with different rules tailored to four levels of risk: unacceptable, high, limited, and minimal risk. At the highest level of risk are systems that conflict with European values and are thus prohibited. Such a ban is a victory to all digital human rights advocates and delivers a strong message: First, do no harm. High-risk systems cover a variety of applications where foreseeable risks to health, safety, or fundamental rights demand specific care and scrutiny. According to the Commission’s impact assessment, roughly 5-15% of all AI systems would fall into this such high-risk category³³. Limited risk systems are those that interact with natural persons and therefore require specific transparency measures to maintain

²⁹ [A European approach to Artificial intelligence](#)

³⁰ [Impact assessment accompanying the AIA](#), p.70

³¹ [European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics \(2015/2103\(INL\)\)](#)

³² E.g. A report ‘[Ethics Guidelines for Trustworthy Artificial Intelligence](#)’ by EU AI HLEG and [European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies \(2020/2012\(INL\)\)](#)

³³ AIA Impact Assessment, p. 71

continued human agency and to avoid deceptive uses. The remaining AI systems – that is to say 70 – 95% fall within the lowest risk category and therefore are not relevant for the AIA since “they represent little or no risk for citizens’ rights or safety”³⁴ and for which the AIA introduces no new rules.

Proportionality. The AIA makes an attempt to have the requirements rightly sized in relation to the potential risks, and to regulate only what is necessary. In the AIA, the Commission presently claims to address proportionality primarily via the just-discussed risk-based approach and varied requirements depending on the system risk level. The majority of AI systems in the market would face only basic transparency requirements as mandatory if any.

Accountability of AI supply chain, ie. providers and deployers, not the end-users. Another incredibly important characteristic of the proposal is how it creates a ground for significant improvements in the supply chain transparency and accountability. No end-user can realistically be expected to take responsibility for evaluating the trustworthiness of complex technology products such as AI products. In order to do so, one would need a good level of transparency to the workings of the system and the technical skills necessary for meaningful evaluation. From this perspective, the Commission’s choice to focus on the accountability of providers, developers, and deployers seems sensible, even if it may have led to some compromises on the end-user transparency obligations. This provider-deployer dualism is also important taking into consideration that 60% of organisations report “Purchased software or systems ready for use” as their sourcing strategy for AI³⁵.

The AIA does not suggest mechanisms that allow individual persons to submit complaints about their concerns and harm caused by AI. This has raised concerns by some. However, the choice seems logical considering that proper evaluation of system conformity would require much more information and technical evaluation skills than what will be available for end-users.

The solution the AIA proposes is the following: Providers are required to set up a post-market monitoring system for actively and systematically collecting, documenting, and analysing data provided by deployers or collected otherwise on the performance of high-risk AI systems on the market. Deployers of such systems are obligated to monitor and report potential situations presenting risks. To support this mechanism’s function, it seems likely that providers and deployers will implement feedback channels or contact points also for the end-users. In addition, similar feedback channels should be expected from national market surveillance authorities to support their role in identifying potential incidents outlined in Article 65.

Meaningful documentation requirements aligned with engineering best practices. The transparency documentation requirements are as follows: Risk management system; Data and data governance; Technical documentation; Record-keeping; Transparency and provision of information to deployers. Such documentation is in the interest of developers for their own record keeping and hope for maintenance. While historically some companies were fooled into expensive maintenance contracts by having been persuaded “not to waste money” on also purchasing the source code from their software suppliers, there can really be no excuse for contemporary corporate boards not to know the importance of documenting the security and capacities of their software including AI systems.

Contextual transparency reporting to AI end-users. While the main focus of the proposal is in setting specific requirements for high-risk AI systems, it is also worth mentioning what is laid down regarding

³⁴ European Commission Press Release: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682)

³⁵ [European Commission, Ipsos Survey, European enterprise survey on the use of technologies based on artificial intelligence, 2020](#), p.53

transparency obligations of systems that interact with natural persons. In a short article (52) the AIA addresses what has become a major challenge with the GDPR informing practices (privacy policies): they're out of context. The requirement of the AIA is focused on the actual use context. It requires that an end-user is made aware of interacting with an AI system. This may well mean that industry standards around labelling AI products will finally start to emerge as providers begin to mark their end-user interfaces accordingly. Moreover, the AIA requires the deployers of emotion intelligence, biometric categorization, and deep fake systems to inform natural persons of their exposure to such AI systems.

Ideally, the AIA might become a new vanguard for transparency more generally. Again, taking proportionality into account, companies and other organisations may choose to expose not only the minimal amount of transparency required by the law (e.g., whether the system deploys AI) but also other aspects of their transparency documentation. This should probably be done in a hierarchical way so that ordinary end-users are not overwhelmed by complexity, nor are small companies required to maintain multiple different types of documentation (which would almost certainly soon fall out of synchronisation). But where providers are comfortable exposing the capacity to "drill down" into the same documentation used for regulatory and other purposes, they may find that they facilitate trust in or engagement with those systems. Some public authorities have already started to implement such transparency via public AI registers, as also recommended by the Commission in the coordinated plan for AI³⁶.

By its proposal, the Commission has shown a way to manage AI-related risks to health, safety, fundamental rights, and even social stability in a way that has all the means to incentivize the industry to take appropriate action. This is of fundamental importance, offering an opportunity towards governance efficiency in regulating technologies of which influences, and impacts will be significant, but are already substantial though perhaps under-recognised. We do expect, however, that the Commission will address the important omission in the AIA - of a channel whereby consumers who have been negatively affected by AI systems can raise their concerns - in its upcoming Civil Liability regime proposals.

Conclusions

The goal of this chapter has been to provide a comprehensive overview of the current situation, understandings, views, values, and regulatory approaches toward AI being deployed and under construction within the European Union with a view towards wider transnational governance of AI systems. Given the Union's acknowledged leadership in this area, we feel this review should be of significant global value. However, we should not overlook digital regulatory advances being made not only in individual American states like California well known for their software industry, but also more widely, including the US state of Illinois which showed leadership on facial recognition, and Asian nations such as China, India, South Korea, and Singapore. China in particular has also just as the time of writing released an enormous slew of AI regulations that are in many ways in keeping with or even extending from the principles described here, as the Chinese government too seeks not only legitimacy with its own population, but also power to control its domestic software corporations.

While our review represents a comprehensive overview of the current state of the art, we must acknowledge that regulation, society, technology, and indeed the global ecological and therefore political-economic context are all highly dynamic. Nevertheless, some things that are unlikely to change, such as the critical role of regulation to stability and well-being, and of the state in enforcing

³⁶ [Coordinated Plan on Artificial Intelligence 2021 Review by the European Commission](#)

such regulation. Artificial Intelligence and other disruptive technologies must be regulated, and such regulation must be coordinated and enforced by the state. This is neither a radical nor overly ambitious viewpoint as some (e.g., large private sector corporations) may argue. One of the primary roles of the state — arguably its very definition — is to establish and ensure quality of life and security for its citizens and residents. Clear, enforceable, and sound regulation and governance enforcement mechanisms are key to this.

As we discussed above, one highly salient but not necessarily unique aspect of AI and its regulation is the importance of global or at least transnational approaches and coordination. This becomes increasingly relevant when it comes to issues such as data sovereignty, social influences, and taxation. While it is unlikely and perhaps undesirable to see complete international harmonization of AI regulations at the governmental level, this chapter has highlighted how, via a process known as the ‘Brussels effect’, a well-coordinated bloc of nations with shared interests may both directly and indirectly, influence regulation internationally. If companies want to build and use AI solutions in the EU, they must comply with EU regulations, and, in many cases, the changes to their business processes may well permeate throughout their other markets. This is not only because these changes are costly, but also because they are widely perceived as providing real, positive value, including economically. It should be said that similar effects can also be observed for Beijing and Washington, though some of the Washington impacts may have been overlooked or taken for granted. But China’s efforts to control what is and is not sold and operated within its national borders has also driven considerable developer effort and corporate concern in non-Chinese corporations, which has drawn the attention of legislators as well world-wide.

While the first transnational bespoke AI regulation is still at least a year from completion, it is of course not possible to fully predict what effect it will have globally. Yet based on previous experience with other fundamental rights-based standards and regulations, it is certainly possible to speculate that the forthcoming EU law may well have a large net positive impact for global society. More generally, regulatory activity in many regions, including the GDPR, is becoming both better informed and better understood. As such, there is good hope that it can be also better coordinated for common good, even if it remains not only varied, but necessarily driven by varied regional regulatory needs.

Bibliography

AlgorithmWatch. (2020). *Automating Society Report* 2020
<https://algorithmwatch.org/en/automating-society-2020/>

Anderson, David and Murphy, Cian C., *The Charter of Fundamental Rights: History and Prospects in Post-Lisbon Europe* (March 31, 2011). EUI Working Papers Law 2011/08, Available at SSRN: <https://ssrn.com/abstract=1894386>

Artificial intelligence: OECD Principles on AI. OECD. <https://www.oecd.org/going-digital/ai/principles/>

Baumeir, Kalomeni, Campbell-Verduyn, Lenglet, Natile, Papin, Rodima-Taylor, Silve and Zhang, 2020. “Global Regulations for a Digital Economy: Between New and Old Challenges,” *Global Policy*, London School of Economics and Political Science, vol. 11(4), pages 515-522, September.

Blankert, A., and Jaurisch, J (2021, January 14). “What the European DSA and DMA proposals mean for online platforms” *The Brookings Institute* <https://www.brookings.edu/techstream/what-the-european-dsa-and-dma-proposals-mean-for-online-platforms/>

Breton, Thierry [@ThierryBreton]. (2021, January 10) *A dogma has collapsed. Platforms no longer hide their responsibility by arguing that they merely provide hosting services. Capitol Hill is the 9/11 of social media.* Op-ed @POLTICO [Tweet]. Twitter.
<https://twitter.com/ThierryBreton/status/1348340670856093696>

Bradford, A., Exporting standards: The externalization of the EU's regulatory power via markets. *International Review of Law and Economics* (2014), <http://dx.doi.org/10.1016/j.irle.2014.09.004>

Bradford, A. (2020). *The Brussels Effect: How the European Union rules the world*. New York: Oxford University Press.

Bryson, J. J. (2019). The Past Decade and Future of AI's Impact on Society. In *Towards a New Enlightenment? A Transcendent Decade*. BBVA Open Mind Series
<https://www.bbvaopenmind.com/en/books/towards-a-new-enlightenment-a-transcendent-decade/>

Bryson, J. J., (2020, June 17) Regulating AI as a pervasive technology: My response to the EU AI Whitepaper Consultation [Blog Post]. Retrieved from <https://joanna-bryson.blogspot.com/2020/06/regulating-ai-as-pervasive-technology.html>

Bryson, J. J. (2017) "The meaning of the EPSRC principles of robotics." *Connection Science* 29, no. 2 p. 130-136.

Brundage, M., & Bryson, J. J. (2016). Smart policies for artificial intelligence. arXiv preprint arXiv:1608.08196.

Crootof, Rebecca and Ard, BJ, Structuring Techlaw (December 18, 2020). *Harvard Journal of Law & Technology*, Forthcoming, Available at SSRN: <https://ssrn.com/abstract=3664124> or <http://dx.doi.org/10.2139/ssrn.3664124>

Echikson, W., (2017, April 13). *Limited liability for the net? The Future of Europe's E-Commerce Directive*. CEPS. <https://www.ceps.eu/ceps-publications/limited-liability-net-future-europes-e-commerce-directive/>

EDRI, (2020, December 18). "The EU's attempt to regulate Big Tech: What it brings and what is missing" <https://edri.org/our-work/eu-attempt-to-regulate-big-tech/>

Erdelyi, Olivia Johanna and Goldsmith, Judy, Regulating Artificial Intelligence: Proposal for a Global Solution (February 2, 2018). 2018 AAAI/ACM Conference on AI, Ethics, and Society (AIES '18), February 2--3, 2018, New Orleans, LA, USA doi/10.1145/3278721.3278731, Available at SSRN: <https://ssrn.com/abstract=3263992>

European Commission (2020). *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/info/sites/info/files/proposal_for_a_regulation_on_a_single_market_for_digital_services.pdf

European Commission, (2021, March 26). Speech by Commissioner Reynders at American Chamber of Commerce on the Digital Transatlantic Economy. “Check against delivery”. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_1482

European Commission (2021) *Study supporting the impact assessment of the AI regulation* <https://digital-strategy.ec.europa.eu/en/library/study-supporting-impact-assessment-ai-regulation>

European Commission, (2020, December 15). Digital Markets Act: Ensuring fair and open digital markets [press release] https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2349

European Commission. (2020, December 15). *Digital Services Act – Questions and Answers* [Press Release] https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348

European Commission. (2020). On Artificial Intelligence – A European approach to excellence and trust [White paper]. Brussels: European Commission. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

European Commission. (2020, December 3). *European Democracy Action Plan: making EU democracies stronger* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2250

European Commission. (2020, December 15). *Digital Markets Act: Ensuring fair and open digital markets* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2349

European Commission (2017, January 10). *Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World* [Communication] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN>
EU Fundamental Rights Agency (2020) *Getting the Future Right: Artificial Intelligence and fundamental right* https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_en.pdf

EU High-Level Expert Group AI (2019). “AI HLEG Update”. <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30466#:~:text=%E2%97%A6%20Definition%20of%20A.I.%3A%20%E2%96%AA,collected%20structured%20or%20unstructured%20data%2C>

European Parliament. (2017). *Report with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market*. https://www.europarl.europa.eu/doceo/document/A-9-2020-0181_EN.html

Evans, B. (2020, July 23). Regulating Technology. *Benedict Evans* <https://www.ben-evans.com/benedictevans/2020/7/23/regulating-technology>

Fioretti, J., (2016, June 6). *German privacy regulator fines three firms over U.S. data transfers*. Reuters. <https://www.reuters.com/article/us-germany-dataprotection-usa-idUSKCN0YS23H>

G20 AI Principles. G20. <https://www.g20-insights.org/wp-content/uploads/2019/07/G20-Japan-AI-Principles.pdf>

Harari, YN (2021, February 26). "Lessons from a year of Covid". *The Financial Times* <https://www.ft.com/content/f1b30f2c-84aa-4595-84f2-7816796d6841>

Jobin, A., Ienca, M. & Vayena, E. The global landscape of AI ethics guidelines. *Nature Machine Intelligence* 1, 389–399 (2019). <https://doi.org/10.1038/s42256-019-0088-2>

Lauchlan, S., (2020, January 23). WEF 2020 - there is no 'Plan B' if time runs out on a global deal on digital services taxation, admits OECD. *diginomica*. <https://diginomica.com/wef-2020-there-no-plan-b-if-time-runs-out-global-deal-digital-services-taxation-admits-oecd>

Lorenz, Philippe, AI Governance Through Political Fora and Standards Developing Organizations — Mapping the Actors Relevant to AI Governance (September 14, 2020). Mapping AI Governance Fora, 2020, Available at SSRN: <http://ssrn.com/abstract=3731354>

Lynskey, Orla, Extraterritorial Impact in Data Protection Law through an EU Law Lens (August 15, 2020). Brexit Institute Working Paper Series - No 8/2020, Available at SSRN: <https://ssrn.com/abstract=3674413>

Mărcuț, M. (2017). *Crystalizing the EU Digital Policy: Exploration into the Digital Single Market*. Springer

OECD, (2019, May 22) "Artificial intelligence – OECD Principles on AI" <https://www.oecd.org/going-digital/ai/principles/>

OECD/C/MIN (2019)3/FINAL *Recommendation of the Council on Artificial Intelligence* <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#dates>

Pfeiffer, S and Carr, R, "Error 404 – Trust Not Found: A European Survey on Digital (Dis)trust," Munich: Munich Security Conference, Munich Security Brief 2, March 2021, <https://doi.org/10.47342/REFQ1817>.

Preusse, Verena and Purnhagen, Kai Peter and Dries, Liesbeth, The 'Brussels Effect' in Action: Do the EU's Standards Travel Abroad? A Study on Control Systems for Geographical Indications in the EU and Thailand (September 3, 2020). Bayreuth Working Paper Series Food Law 02/2020, Forthcoming, Available at SSRN: <https://ssrn.com/abstract=3685915>

Ram, N., & Gray, D. (2020). Mass surveillance in the age of COVID-19. *Journal of law and the biosciences*, 7(1), Isaa023. <https://doi.org/10.1093/jlb/Isaa023>

Rességuier, A., & Rodrigues, R. (2020). AI ethics should not remain toothless! A call to bring back the teeth of ethics. *Big Data & Society*, 7. <https://journals.sagepub.com/doi/full/10.1177/2053951720942541>

Schiff, D., Biddle, J., Borenstein, J., & Laas, K. (2019, December 18). What's Next for AI Ethics, Policy, and Governance? A Global Overview. <https://doi.org/10.1145/3375627.3375804>

Schwartz, Paul M., Global Data Privacy: The EU Way (October 10, 2019). Paul M. Schwartz, Global Data Privacy: The EU Way, 94 New York University Law Review 771 (2019), Available at SSRN: <https://ssrn.com/abstract=346554>

Schwartz, Paul M. and Peifer, Karl-Nikolaus, Transatlantic Data Privacy (November 7, 2017). 106 Georgetown Law Journal 115 (2017), UC Berkeley Public Law Research Paper, Available at SSRN: <https://ssrn.com/abstract=3066971>

Shalal, A., Nienaber, M., and Thomas, L., (2021, February 26). *U.S. drops 'safe harbor' demand, raising hopes for global tax deal*. Reuters. <https://www.reuters.com/article/us-g20-usa-oecd-idUSKBN2AQ2E6>

Silver, L., (2018, August 17) *How Americans and Western Europeans compare on 4 key social and political issues*. Pew Research Center. <https://www.pewresearch.org/fact-tank/2018/08/17/how-americans-and-western-europeans-compare-on-4-key-social-and-political-issues/>

Singel, R., (2008, April 8). *EU Tells Search Engines to Stop Creating Tracking Databases*. WIRED. <https://www.wired.com/2008/04/eu-tells-search/>

Stix, Charlotte, Actionable Principles for Artificial Intelligence Policy: Three Pathways (February 19, 2021). Sci Eng Ethics 27, 15 (2021), Available at SSRN: <https://ssrn.com/abstract=3792370>

Veale, Michael and Zuiderveen Borgesius, Frederik, Demystifying the Draft EU Artificial Intelligence Act (July 31, 2021). Computer Law Review International (2021) 22(4), Available at SSRN: <https://ssrn.com/abstract=3896852>

Vestager, M., and Borrell, J., (2021, March 10). Why Europe's Digital Decade Matters. Project Syndicate. <https://www.project-syndicate.org/commentary/europe-digital-decade-by-margrethe-vestager-and-josep-borrell-2021-03?barrier=accesspaylog>

Venkataramakrishnan, S., (2020, April 27). GDPR accused of being toothless because of lack of resources. <https://www.ft.com/content/a915ae62-034e-4b13-b787-4b0ac2aaff7e>

Whittlestone, J., Nyrop, R., Alexandova, A. and Cave, S, 2019. The Role and Limits of Principles in AI Ethics: Towards a Focus on Tensions (January 2019), (AIES '19): Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics and Society, January 2019. 195-200 <https://dl.acm.org/doi/10.1145/3306618.3314289>

Wu, T. (2018). The curse of bigness. Antitrust in the new guilded age. Columbia Global Reports.