



# Sociotechnical imaginaries of algorithmic governance in EU policy on online disinformation and FinTech

new media & society  
2022, Vol. 24(4) 942–963  
© The Author(s) 2022



Article reuse guidelines:  
sagepub.com/journals-permissions  
DOI: 10.1177/14614448221079033  
journals.sagepub.com/home/nms



**Mariëlle Wijermars**   
Maastricht University, The Netherlands

**Mykola Makhortykh**   
University of Bern, Switzerland

## Abstract

Datafication and the use of algorithmic systems increasingly blur distinctions between policy fields. In the financial sector, for example, algorithms are used in credit scoring, money has become transactional data sought after by large data-driven companies, while financial technologies (FinTech) are emerging as a locus of information warfare. To grasp the context specificity of algorithmic governance and the assumptions on which its evaluation within different domains is based, we comparatively study the sociotechnical imaginaries of algorithmic governance in European Union (EU) policy on online disinformation and FinTech. We find that sociotechnical imaginaries prevalent in EU policy documents on disinformation and FinTech are highly divergent. While the first can be characterized as an algorithm-facilitated attempt to return to the presupposed status quo (absence of manipulation) without a defined future imaginary, the latter places technological innovation at the centre of realizing a globally competitive Digital Single Market.

## Keywords

Algorithmic governance, digital policy, disinformation, European Union, FinTech, sociotechnical imaginaries

## Corresponding author:

Mariëlle Wijermars, FASoS, Maastricht University, P.O. Box 616, 6200 MD Maastricht, The Netherlands.  
Email: [m.wijermars@maastrichtuniversity.nl](mailto:m.wijermars@maastrichtuniversity.nl)

## Introduction

Algorithmic systems increasingly affect the governance of key functional elements of society, including transportation, communication and law enforcement. By enabling private corporations and state authorities to make use of unprecedented volumes of data and automate decision-making processes, algorithms can enable more efficient performance (Olhede and Rodrigues, 2017). At the same time, the ongoing algorithmization of governance raises concerns about potential negative effects that algorithmic biases or manipulations can have on individual citizens' rights and the functioning of societal institutions (McGregor et al., 2019). These concerns are amplified by the frequently 'closed box' nature of algorithmic systems (Pasquale, 2015) that limits public understanding of their functionality (Carlson, 2017; Olhede and Rodrigues, 2017).

Much essential work has been done on algorithmic governance – complementing theorization (Coglianese and Lehr, 2019; Katzenbach and Ulbricht, 2019; Latzer and Festic, 2019) with in-depth empirical scrutiny of algorithmic systems and their effects in various societal domains (Bellanova and De Goede, 2022; Möller et al., 2018; Noble, 2018; Makhortykh et al., 2020). While scholars often point out that there are similarities between sectors where algorithmic systems are employed, comparative studies are sparse. We argue that comparative approaches are needed to grasp the context specificity of how algorithmic governance is understood, as well as to question the assumptions on which its evaluation within different domains is based.

With regard to public administration's focus on single policy areas, scholarship is at risk of mirroring how policymaking itself has not yet sufficiently caught up with the fact that datafication blurs distinctions between policy fields and that regulatory effects extend beyond sectors. In finance, for example, algorithms are used in credit scoring while money has transformed into transactional data that large data-driven companies, including social media platforms, seek to capitalize on (Westermeier, 2020). Meanwhile, financial technologies (FinTech) are emerging as a new locus of information warfare, for example, through their interplay with social media that are utilized for spreading disinformation (Di Pietro et al., 2021). The aim of this article, then, is to examine how challenges and risks associated with algorithmic governance are imagined and narrated in the context of two priority areas of European Union (EU) policymaking: online disinformation and FinTech. Applying the concept of sociotechnical imaginaries (i.e. collective imaginations of the intersections between social life and/or order and technological projects; Jasanoff and Kim, 2009), we study the conceptualization of the present and future role of algorithmic systems in the respective domains.

In addition to the connections between social media platforms and financial services already mentioned, we selected these policy issues because, first, information security and finance are the two domains where the use of algorithms is particularly pervasive, while it simultaneously has the potential to affect citizen rights. In content moderation on social media platforms, the increasing use of automated systems enables effective detection and countering of adversarial activities (e.g. disinformation campaigns), whereas in finance the deployment of algorithms and big data enables unprecedented possibilities for scaling and accelerating financial operations and generating predictive assessments. The risks associated with possible algorithmic errors

(e.g. misclassification of true content as false), exploitation of vulnerabilities (e.g. breaching integrity of online financial operations) and assumed validity of predictive assessments are also high. The fields are also similar in the sense that algorithmic systems are, or can be, simultaneously part of the problem, the regulatory response *and* the compliance mechanism put in place to monitor this response, as will be elucidated below. This complexity creates particular regulatory challenges.

Finally, while some of the factors mentioned above can also be applied to other areas in which algorithmic systems are increasingly deployed (e.g. self-driving cars), disinformation and FinTech stand out for being profoundly transnational policy issues. Multilevel governance poses particular challenges for state efforts to understand, manage and restrict the increasing implementation of forms of algorithmic governance in both national and transnational domains (Saurwein and Spencer-Smith, 2020) and necessitates the creation of complex data infrastructures for the enactment of algorithmic regulation (Bellanova and De Goede, 2022). Today, online disinformation and FinTech are per se transnational policy issues that require intense interstate and multistakeholder cooperation to effectively deal with the associated threats. While the deployment of (other) algorithms is often envisioned as part of the solution to do so, this, in turn, raises its own challenges – varying from the need for establishing reliable data exchange channels to the alignment of algorithmic models used to detect threats, or the development of means of interstate algorithmic audit (Mittelstadt, 2016). In selecting these domains, our study also positions itself within the emerging debate on the similarities between both spheres (e.g. the platformization of finance; Langley and Leyshon, 2021; Westermeier, 2020) and on ‘how the key theories underpinning financial services regulation could engender policy solutions’ to better address ‘the role played by content recommender systems in compounding the policy problem of disinformation online’ (Bennett, 2021).

The article is structured as follows. We first discuss in further detail what is meant by algorithmic governance and how it manifests itself in relation to online disinformation and FinTech. Then, we provide an overview of EU policymaking concerning the regulation of online content and innovative digital financial services. Subsequently, we explain the methodology and corpus selection of the study. The remaining sections present the results of the empirical analysis.

## **Algorithmic governance**

### ***Defining algorithmic governance***

Algorithms are computer-based epistemic procedures (Katzenbach and Ulbricht, 2019) that, by utilizing the properties of the large volume of available data (i.e. their volume, variety and velocity; Sivarajah et al., 2017), facilitate automation of processes, varying from traffic regulation to news distribution and criminal justice. By doing so, algorithms enable the functionality of complex decision-making systems that affect many aspects of modern societies, from individual daily routines (Latzer and Festic, 2019) to broad institutional practices (Latzer et al., 2016). Consequently, the increasing deployment of algorithmic systems causes numerous societal changes, such as the elimination and formation of types of jobs or the transformation

of existing power relations within organizations and institutions. In addition, they influence ‘existing modes of governance and foster novel power relations among public and private actors’ (Bellanova and De Goede, 2022: 2).

The diverse societal effects of algorithmic systems raise the need for their critical assessment and the implementation of measures to rein them in. This need is increasingly addressed by the research agenda on algorithmic governance (see, e.g. Coglianese and Lehr, 2019; Danaher et al., 2017; Festic, 2022; Gritsenko and Wood, 2022; König, 2020; Sætra, 2020). Commonly understood as the use of digital technologies (in particular, those related to artificial intelligence [AI] and big data) for implementing different forms of social ordering (Katzenbach and Ulbricht, 2019), the concept of algorithmic governance is adopted by different disciplines, ranging from law (e.g. Kalpokas, 2019; Larsson, 2018) and media studies (e.g. Gorwa et al., 2020; Müller-Birn et al., 2013; Napoli, 2015) to political science (e.g. Graaf, 2018) and science and technology studies (e.g. Brown, 2020), for studying the broad range of issues associated with the adoption of algorithm-driven decision-making systems.

Two branches of research that are particularly pronounced concern the use of algorithms as a form of regulation for social ordering (i.e. governance *by* algorithms) and the regulation of algorithmic systems of decision-making themselves (i.e. governance *of* algorithms). Research of the former branch usually focuses on ‘intentional and unintentional steering effects’ (Latzer and Festic, 2019: 2) of algorithmic systems as well as their different forms, ranging from automated content moderation by online platforms (Gorwa et al., 2020) to predictive policing (Bennett Moses and Chan, 2018). By contrast, governance *of* algorithms scholarship discusses how the complexities involved in regulating processes of algorithmic decision-making should be addressed, in particular the need to make them transparent (Coglianese and Lehr, 2019), accountable (Katzenbach and Ulbricht, 2019) and fair (Bellanova and De Goede, 2022). The usual lack of transparency (Pasquale, 2015) is among the most acknowledged challenges of algorithmic decision-making and its regulation. While it is clear that algorithmic systems should be transparent enough to be accountable (‘auditable’), the exact implementation of and standards for algorithmic transparency remain debated. The security risks associated with making more information about a system’s functionality available to potential attackers further complicate the process of making algorithmic governance systems more transparent.

While the distinction between governance *by* and *of* algorithms is useful for organizing the discussion on the conceptual level, it is also misleading. Because of the complexity of algorithmic systems, the use of algorithms as regulatory devices (i.e. governance *by* algorithms) rather presumes that such regulation will be monitored and controlled by other algorithms (i.e. governance *of* algorithms), thus leading to what Eagle (2001) has called ‘a spiral of regulation’: a situation, in which the growing number of mechanisms for algorithmic governance prompts the need for even more mechanisms used to regulate the former mechanisms (p. 914). The algorithmic spiral of regulation complicates the differentiation between different forms of algorithmic governance. In this article, we therefore propose to go beyond the dichotomous interpretation of algorithmic governance and instead approach it as a complex phenomenon that encompasses both aspects. The fact that policy documents do not necessarily differentiate between the two dimensions and, instead, often treat them together reinforces this choice.

A key contribution that we aim to make concerns the lack of comparative research of algorithmic governance. While general issues of algorithmic decision-making, such as the lack of transparency, have been widely studied (e.g. Coglianese and Lehr, 2019; Katzenbach and Ulbricht, 2019; Pasquale, 2015), the universality versus context dependency of algorithmic governance remains underexplored. Algorithmic governance tends to be studied and theorized within the context of a particular sphere where algorithmic systems are applied (e.g. news distribution [Helberger, 2019] or law enforcement [Wisser, 2019]) and is usually approached from a single disciplinary perspective (e.g. political science or law). Comparative studies – analysing algorithmic governance in different geographical contexts, across multiple online platforms or in different sectors – remain rare. This fragmentation and lack of progress towards a better understanding of the context-determined differences is exacerbated by the fact that some applications and contexts receive great scholarly and public attention, while others are neglected.

The final aspect of algorithmic governance scholarship we aim to address is the understudied nature of the long-term societal consequences of the use of algorithmic systems and the ways they enable new forms of social ordering. The frequent focus on short-term effects of algorithmic systems and their regulation makes it harder to assess to what extent the actual output of the governance system corresponds with its intended output and complicates the evaluation of normative aspects of algorithmic governance. This lack of awareness, we suggest, is particularly damaging in policymaking. Without accounting for the long-term consequences and possible futures enabled by algorithmic systems, regulation is limited to short-sighted interventions rather than future-oriented policymaking. Scholarship, journalistic reporting and policymaking oriented on the present condition can factor into the creation of moral panics (Bruns, 2019) and can result in policies aimed at blocking certain effects of algorithmic systems ('damage control') rather than looking for ways to realize their desired performance. We therefore set out to investigate to what extent the long-term effects of algorithmic governance in the two areas are acknowledged in policy documents and whether they promote future imaginaries of the preferred functioning of algorithmic decision-making, which, we argue, is more optimal as it guides further policymaking efforts and facilitates impact assessment.

### *Algorithmic governance, disinformation and FinTech*

The shift towards using algorithmic systems as part of governance and the associated changes in scope, complexity and automatization of governance-related processes prompt a re-assessment of the difference between earlier expert-based governance and new systems shaped by algorithms and big data (Campbell-Verduyn et al., 2017). In the case of both disinformation and FinTech, algorithmic systems simultaneously serve as regulatory mechanisms and major challenges to these mechanisms.

With regard to disinformation, algorithmic systems are commonly referred to as a key means of addressing the unprecedented volume of false or misleading information affecting the public sphere. Because of the volume and speed of distribution of online disinformation, both within the confines of and across platforms, human curators are

not capable of culling its spread and have to rely on algorithmic solutions, such as automated content curation systems (Gorwa et al., 2020) or AI-driven disinformation detection mechanisms. The need for these solutions is amplified by the fact that algorithms themselves are among the main drivers of the ongoing ‘infodemic’ as they are used to programme and deploy automated agents (bots) that disseminate false information.

The increasing deployment of algorithmic systems to counter both human- and algorithm-driven disinformation raises multiple challenges from the perspective of algorithmic governance. In addition to the substantial complexity of algorithmic systems employed against disinformation, there are ethical concerns related to their use, ranging from their potential to limit free speech (consciously or because of false positive errors) to the appropriateness of regulating human communication via non-human agents (Marsden et al., 2020). These concerns are exacerbated by the frequent lack of transparency (Pasquale, 2015) on the part of platforms and the difficulties of communicating the principles behind their functionality to platform users without increasing security risks by making more information available to potential attackers.

Compared to the disinformation domain, the field of FinTech features more academic studies dealing explicitly with the question of algorithmic governance. This difference can be explained by the extensive integration of big data routines in global finance, where the use of algorithmic systems has been viewed as a competitive edge since the early 2010s (Campbell-Verduyn et al., 2017) while it has also been central to (international) regulatory efforts, for example, to counter terrorism financing (De Goede, 2012). Simultaneously, the growing use of algorithms in FinTech raises concerns about how it might challenge existing market regulation and control mechanisms (Gruin, 2019). Increasingly, FinTech takes on the characteristics of a ‘platform political economy’ as it, for example, ‘aggregate[s] and monetise[s]’ the ‘[t]ransaction data produced by digital and mobile payments’ (Langley and Leyshon, 2021: 377).

The diversity of governance-related functions performed by algorithmic systems in the field of FinTech can be captured in a three-part framework (Campbell-Verduyn et al., 2017): governance through, with, and by algorithms. The first layer of governance focuses on the use of algorithms as a means of facilitating governance procedures (e.g. by informing experts who make the final decision as in the case of credit scoring). The second layer assigns higher weight to the input of algorithmic systems (e.g. in the case of bank capital adequacy measurement). Finally, the third layer assumes that algorithmic systems have a high degree of independence in making and then enforcing decisions (e.g. by initiating buy/sell orders in the context of financial trading).

Despite the fact that disinformation and FinTech may appear disparate at first glance, we argue that the application of algorithmic systems in these two cases should be seen not as opposing, but as related phenomena. In both domains, there is a mismatch between the use of algorithms for tackling specific tasks (detecting disinformation or money laundering) and the governance of such uses, in particular in those cases, when algorithmic systems are delegated a high degree of independence. Second, as will be discussed in further detail below, regulators in both domains struggle with how to respond to the expansion of big tech and the diversification of services offered by their respective digital ecosystems.



## EU policymaking in the digital domain

As developments in information and communication technologies (ICTs) affect many policy fields, the EU has been involved in their regulation for several decades. In parallel with the proliferation of Internet access in its Member States and the boom in the development of digital technologies, the digital domain has become a key priority for the European Commission, who is eager to simultaneously stimulate innovation and address concerns of information security, cybercrime, the dissemination of terrorist propaganda and various other online harms (Mansell, 2014). Algorithms are being implemented in ever more domains and are changing sector dynamics. Wide-ranging in their application and effects, some of these innovations require updates to or new EU policy to be developed. The sections below provide an overview of EU regulatory involvement in the two domains examined in this article: disinformation and how it is addressed through content moderation on online platforms and FinTech.

### *Content moderation on online platforms: from terrorist propaganda to disinformation*

The operations of algorithmic systems on online platforms – from online retail and services to social media – have attracted the interest of EU policymakers in multiple ways. Concerns about unfair competition emerged regarding product comparison and retail websites (e.g. regarding personalized pricing; Townley et al., 2017) as well as search engines (Kucharczyk, 2019). While algorithmic governance-related issues have mostly pertained to, or been approached as, issues under EU competition law and inhibitors of the development of the Digital Single Market (DSM), more recently, the debate on monopolization (especially by US firms) has acquired significant security undertones.

With regard to social media platforms, our review of recent policy initiatives showed that the EU debate on algorithmic governance is twofold: first, it concerns the question how platforms moderate user-generated content; second, it concerns the impact of the algorithmic recommender systems used by these platforms on political deliberation and news consumption, including their potential polarizing effects. Calls for social media to remove certain types of content evolved over time to highlight particular types of harmful information. These include copyright infringement, terrorist and extremist content and most recently disinformation. Given the scale of their operations, machine learning has been extensively used to search for, identify and remove harmful content, complementing the flagging of content by users (Gorwa et al., 2020). The lack of contextual sensitivity of automated content moderation has, however, attracted criticism in its own right. Many caution that the EU's self-regulatory approach will result in overmoderation by platforms and thereby damage freedom of expression, among other rights (Riis and Schwemer, 2019). In addition to policy aiming to limit the spread of illegal or harmful content online, there has been concern about the role of social media's recommendation systems in creating or exacerbating societal divides and amplifying the spread of, for example, disinformation.

Disinformation first solicited an EU response in 2014 in relation to accusations of Russia engaging in 'information warfare' in the conflict in Ukraine (Saurwein and

Spencer-Smith, 2020). While information interference was, at first, mostly on the radar of states in Russia's 'sphere of influence', it gained political prominence after Russian attempts at election interference – seeking to manipulate public opinion and electoral outcomes through information campaigns on social media – during the 2016 US presidential elections. In preparation of the 2019 EU parliamentary elections, a high-level expert group on fake news and online disinformation was established in 2018 and a communication outlining 'a European approach' to tackling disinformation was presented (Saurwein and Spencer-Smith, 2020). The Commission recognized the central position that online platforms occupy where it concerns online disinformation and prioritized self-regulation of its major players. The EU Code of Practice on Disinformation of October 2018 has been the main tool to engage the industry in anti-disinformation efforts. Its signatories, including Google, Facebook and Mozilla, 'commit to making the origin and scale of political advertising more transparent, preventing "fake news" publishers from profiting from advertising revenue and removing fake accounts faster' as well as to 'set clear rules for the misuse of bots on their platforms' (Saurwein and Spencer-Smith, 2020: 6). Beyond sector self-regulation, the EU has supported the creation of a network of fact-checkers and information-sharing initiatives to counter election interference, and invested in promoting media literacy.

How the EU understands the role of online platforms in the production and publication of online content has shifted from one of editorial control – the lack thereof limiting their responsibility for the content – to organizational control – acknowledging that 'platforms selectively promote and remove specific kinds of content [and] [t]hey thereby take over some tasks traditionally exercised by publishers' (Van Drunen, 2020: 1–2). The shift was necessitated by the fact that, under traditional media law, the lack of editorial control translated into no editorial responsibility. This bears similarity to 'a general liability exemption for neutral hosting services that take down illegal content once they become aware of it' (Van Drunen, 2020: 6). As the organization of information, rather its publication, increasingly determines its possible impact, this limited responsibility is increasingly being questioned. The revised Audiovisual Media Services Directive of 2018, for example, 'require[s] platforms to take appropriate measures with regard to content that is illegal, commercial, or harmful to minors' and outlines 'concrete appropriate measures' (Van Drunen, 2020: 11).

Most EU initiatives focus their efforts on protecting the integrity of electoral processes, yet its salience goes beyond elections. The potential social and political damages resulting from incorrect or misleading health information, for example, are a continuous cause for concern. Shielding its citizens from intentionally wrongful or misleading information, spread by state or non-state actors for political, commercial or other aims, has proven to be a challenging task for the EU and its Member States.

Disinformation and its amplification through online platform recommender systems, thus, is seen as a phenomenon that may disrupt democratic processes and undermine societal stability, as well as to make societies more vulnerable to interference by foreign or other mal-intentioned actors. While algorithmic systems may be part of the solution by facilitating automated detection, they are commonly seen as a root facilitator of the problem because of their amplifying qualities (Bradshaw, 2019).



## *From FinTech to TechFins: safeguarding the global competitiveness of Europe's financial sector*

While earlier FinTech adoption tended to be 'driven by incumbent financial institutions' and developed 'in close partnership with regulators', FinTech start-ups entered the field *en masse* following the 2008 Global Financial Crisis (Zetzsche et al., 2018: 400). The acceleration of the use of technology in finance necessitates a 'transit from regulations designed to control human behaviour to a regulator looking at supervising automation processes' (Zetzsche et al., 2018: 400). In its wake, a boom has occurred in the market of technologies that facilitate such regulation, compliance and risk management, active beyond the field of finance, dubbed 'RegTech'.

Policymakers and academics alike voice a drive for innovation to reap the gains of FinTechs and not lose out to international competitors (Zilgalvis, 2014). In the words of Cœuré (2018), a member of the Executive Board of the European Central Bank,

[p]re-emptively drawing in the reins in the name of financial stability could stifle innovation, prevent FinTechs from developing important economies of scale, and deprive small businesses and households of the benefit of technological progress. On the other hand, allowing risks to accumulate in an unregulated sector may undermine financial stability and undo the benefits of past regulatory efforts.

In 2016, the Commission launched an internal FinTech Task Force. Spurred on by the European Parliament, the Commission launched a public consultation in 2017, which resulted in the presentation of the FinTech Action Plan in 2018. The plan built upon and aimed to complement existing regulatory frameworks on, among others, money laundering and terrorist financing (Directive (EU) 2015/849) and consumer financial services (COM (2017) 139).

While algorithmically amplified disinformation on social media at first glance is worlds apart from digital innovation in finance, they have a shared concern that poses a major policy challenge to European policymakers: the expanding influence of Big Tech. As Yves Mersch, a member of the Executive Board of the European Central Bank, explains, FinTech is no longer the exclusive domain of small start-ups. '[H]uge, globally active technology companies, the so-called big tech companies, are also entering the market' and 'their existing customer networks and huge amounts of proprietary data' provide them with competitive advantage in the provision of financial services (Mersch, 2019). Alibaba Group's Ant Financial, which runs Alipay, and Tencent are prominent successful examples of what has come to be known as 'TechFins': technology, telecommunications, e-commerce and other companies that expand into financial services, building upon their 'data-based view of their customers' [. . .] preferences and behaviours' (Zetzsche et al., 2018: 406). TechFins have the potential to outperform banks in some of their core activities (assessment of creditworthiness and risk) and can expand 'related financial service offerings, particularly lending (to consumers and SMEs) as well as cash and investment management' (Zetzsche et al., 2018: 405, 408), thereby entering in direct competition.

The regulatory dilemma, according to Mersch, lies in the fact that while this shift could be beneficial on the consumer end – ‘using predictive algorithms, machine learning and a wider range of data, available from online spending or social media [. . .] big tech could become more efficient at lending than traditional banks’ – negative impacts on the financial system are difficult to predict, yet could be substantial. If their financial activities are predominantly a means of gaining access to more data sources to facilitate the selling of products and services, the expansion of big tech into the market of FinTech ‘could [. . .] increase market concentration by exploiting their [large technology companies] network externalities’ and give rise to novel types of risks. As FinTech adopts the ‘logics and logistics of platforms’, this could lead to them ‘replac[ing] existing retail money and finance markets with newly structured and platformed arrangements that have monopolistic and oligopolistic tendencies’ (Langley and Leyshon, 2021: 377, 382).

Big tech’s involvement may also impede oversight by central banks by ‘shield[ing] payments from the scrutiny of authorities guarding against illegal activities, such as money laundering’ and could entice more risk-taking behaviours in banks as they seek to retain their market positions (Carstens, 2018). In short, ‘a FinTech is a *financial* intermediary while a TechFin is a *data* intermediary’ (Zetsche et al., 2018: 409, italics in original), and this can become problematic since existing regulatory requirements for either sphere may differ. It is only when TechFins have direct access to client funds that they fall under the much stricter financial regulation and monitoring (Zetsche et al., 2018).

A second similarity of the two domains is that both aspects of algorithmic governance – the governance of algorithms and the use of algorithms in governance – are at play. For disinformation, algorithmic recommenders play a role in the spread and amplification of false or misleading information but are also seen as part of the solution (using algorithms and machine learning to detect disinformation and other illegal content). In finance, the possible benefits and efficiency gains from algorithmic systems and machine learning are great – from detecting fraudulent transactions to robo-advice – while associated risks for financial stability and consumer protection, it is believed, may be addressed through improved regulatory oversight by means of even more technological solutions.

## Methodology

We examine EU policy documents dealing with algorithmic governance in the sphere of disinformation and FinTech. We use the concept of sociotechnical imaginaries to scrutinize assessments of the long-term effects of the deployment of algorithmic systems in these two domains and accompanying visions of the future. To implement our study, we utilized document analysis which is a method that is commonly employed for studying sociotechnical imaginaries in domains ranging from nuclear power (Jasanoff and Kim, 2009) to nanotechnology (Burri, 2015). The document analysis is based on the interpretation of the document in the context of a particular subject, in our case algorithmic governance. The chosen approach is based on the assumption that policy documents serve as a primary means of codification as well as promotion of

sociotechnical imaginaries at the institutional level. While the use of a different methodological approach, for instance, interviews, could provide insight into individual perceptions of the sociotechnical imaginaries, we find document analysis to be better suited for studying how interpretations of the future of algorithmic governance are ‘filtered and repackaged into dominant targets of public action and associated public reasoning’ (Jasanoff and Kim, 2009: 123), which is achieved through formal procedures that are established via collective action and codified through documents, rather than determined by individual preferences.

### *Sociotechnical imaginaries*

Constituted by a complex amalgamation of ‘promises, visions and expectations of future possibilities’ (Jasanoff and Kim, 2009), sociotechnical imaginaries influence socio-economic and political environments. By embodying the perceptions of technological promises, and also challenges and threats, they project future goals and map possible ways of attaining these goals for different categories of actors, varying from corporations to governments and the general public. Research shows that sociotechnical imaginaries have ‘the power to influence technological design, channel public expenditures, and justify the inclusion or exclusion of citizens with respect to the benefits of technological progress’ (Jasanoff and Kim, 2009). Groves et al. (2016) show how imaginaries of the future shape, but also constrain choices in relation to specific technological solutions. Similarly, Beckert (2016) stresses the importance of individual and collective perceptions of technological futures that define economic opportunities and risks, thereby constituting the basis of the temporal orientation of the capitalist economy.

Sociotechnical imaginaries are embedded in social organizations and practices and often codified in organizational statements or institutional protocols. Yet, they are more than policy agendas or master narratives. Instead of being articulated via ‘repeated use of words and images in public communicative space’ (Jasanoff and Kim, 2009: 123), future imaginaries are also embodied in power relations and actions, such as the allocation of funds to particular projects. The relationship between sociotechnical imaginaries and power dynamics is also reflected in the unequal standing of different visions of the future: some of them, in particular those backed by powerful institutions, achieve prominence, whereas others remain marginal (Ruppert, 2019).

### *Document selection and analysis*

The corpus was constructed with the aim of optimizing the validity of the comparison. Two key EU policy initiatives introduced in 2018 were taken as the starting point: The Action Plan on Disinformation and FinTech Action Plan. Then, we traced related EU policy activity backward and forward in time to identify policy documents to be added to the corpus. Only documents from the Commission, Council and Parliament were included. While other institutions, such as the Council of Europe and European Central Bank, are also active and (to varying degrees) influential in the respective fields, we chose to exclude them since any differences uncovered by our analysis may then have been caused by the different (types of) institutions behind them. Since algorithmic systems are often referred

**Table 1.** Specification of selected policy documents.

Case	Document	Institution	Year	Codename
Disinfo	European Parliament resolution of 15 June 2017 on online platforms and the digital single market	European Parliament	2017	EPres2017
Disinfo	Action Plan against Disinformation	European Commission	2018	Action2018
Disinfo	Code of Practice on Disinformation	European Commission	2018	Code2018
Disinfo	Communication: Tackling online disinformation: a European Approach	European Commission	2018	Comm2018
Disinfo	Communication: the EU's fight against COVID-19 Disinformation	European Commission	2020	Comm2020
Disinfo	Progress report on the April Communication	European Commission	2018	ProgressReport2018
FinTech	European Parliament resolution of 17 May 2017 on FinTech: the influence of technology on the future of the financial sector	European Parliament	2017	FinEPres2017
FinTech	Consultation document FinTech: A more competitive and innovative European financial sector	European Commission	2017	FinConsultation2017
FinTech	FinTech Action Plan	European Commission	2018	FinAction2018

to by other terms, we manually collected and assessed documents for relevance, rather than rely on keyword searches. Analysing two initiatives of a similar kind (Action Plan) that were developed around the same time supports the comparative dimension of the study. The resulting corpus consists of nine policy documents, listed in Table 1. The limited size of corpus can be explained by the relatively recent rise of interest in the role of algorithms; in the case of disinformation, the role of algorithms in disinformation campaigns began to be recognized during the Ukraine crisis and the series of election interferences in the United States and EU (Ferrara, 2017).

To organize our analysis, we identified three aspects of utilizing algorithmic governance in the disinformation and FinTech domains:

1. *Problem formulation.* The set of challenges/opportunities to be addressed/realized and the ways these challenges/opportunities are affected by algorithms.
2. *Problem solution.* The set of techniques used to tackle the problem and whether these techniques involved the use of algorithms.
3. *Problem outcome.* The visions of the desired outcome of the problem and the ways these visions account for algorithmization.

Following this structure, the sections below present the results of the empirical analysis.

## Case 1: disinformation on social media

### *Problem formulation*

The documents refer to disinformation as a key challenge associated with the growing use of online platforms. The Parliament and the Commission stress the importance of citizens' access to reliable information that can be undermined by 'fake news' (EPres2017) and disinformation (Action2018, Code2018 and Comm2018). We identified substantial changes in how the disinformation problem is formulated: shifting from acknowledging the need to strengthen the response to fake news (EPres2017) to discussing the 'unprecedented infodemic' (Comm2020) caused by the distribution of false information online related to the COVID-19 pandemic.

Starting from the Action Plan, disinformation is increasingly treated as a means by which adversarial agents promote their economic gains or intentionally deceive the public. While doing so, it causes public harm in the form of threats to political and policy-making processes as well as public goods, such as the protection of EU citizens' health, the environment or security (Action2018). In the long term, disinformation can undermine the public debate on which EU democratic societies rely (Code2018; Comm2018) and deprive citizens from access to 'a variety of verifiable information' (Action2018: 1), which is required for expressing political will through free and fair political processes. In the case of the COVID-19 pandemic, disinformation can 'create confusion and distrust and undermine an effective public health response' (Comm2020).

Besides the shift in recognizing the scope and potential detrimental effects of disinformation for the public sphere, the documents show changes in how they define adversarial actors. Following the initial lack of discussion on *who* uses fake news to manipulate the public sphere (EPres2017), later documents focus on 'foreign state actors' and 'third countries' (Action2018: 3) presenting disinformation as part of information warfare. The joint communication on tackling COVID-19 disinformation refers to both foreign and domestic actors utilizing disinformation and attributes particularly intense use of disinformation to Russia and China (Comm2020).

The role of algorithms in the proliferation of disinformation remains largely unspecified. The documents only indirectly mention how deployment of algorithmic systems might facilitate the misuse of platforms for disseminating false information. For instance, there is mention of the misuse of automated bots (Code2018) and the activities of Cambridge Analytica that allowed 'to target the delivery of disinformation content to specific users [...] with the ultimate goal of influencing the election results' (Action2018: 4). Like the Code of Practice, the Action Plan notes the adversarial use of bots 'to spread and amplify divisive content and debates on social media' (Action2018: 4).

### *Problem solution*

The approaches for countering disinformation remain rather declarative. The EU institutions acknowledge the need to 'curb coordinated manipulative behaviour and increase transparency around malign influence operations' and do so 'in full respect of fundamental rights, in particular freedom of expression' (Comm2020). The exact procedure for doing so remains vague. Even in those instances, when more practical suggestions are

given (e.g. to promote authoritative content via online platforms; Comm2020), the exact mechanisms for doing so are unclear.

A recurring issue is the need for more intensive cooperation between civil society, EU institutions, and the private sector, in particular social media platforms (Action2018 and Comm2020). Such cooperation can take the form of improving scrutiny of advertisement placement, increasing transparency of political advertising, avoiding misrepresentation (e.g. in the form of fake accounts) and facilitating academic research. The Action Plan (2018) notes increased media literacy and developing an independent network of fact-checkers as prerequisites for countering disinformation, whereas the joint communication on tackling COVID-19 disinformation (Comm2020) lists the need to inform users about interactions with disinformation.

Algorithms (can) play a substantial role in addressing disinformation, yet are rarely addressed directly: for instance, the Code of Practice (Code2018) notes the importance of the use of verification tools for scrutinizing advertisement placement. Similarly, algorithms should power ‘products, technologies and programs [ . . . ] to help people make informed decisions when they encounter online news that may be false’ (Code2018: 7), but it is never specified. The Action Plan (Action2018: 5) emphasizes the need to develop ‘analytical tools such as dedicated software to mine, organise and aggregate vast amounts of digital data’. It also notes a rapid alert system installed to provide alerts on disinformation campaigns in real-time through a dedicated technological infrastructure, yet does not elaborate on its implementation.

The communication on countering COVID-19-related disinformation (Comm2020) similarly proposes algorithm-based solutions without directly referring to algorithms: prioritizing information from ‘national and EU authorities, as well as professional media’ and ‘inform[ing] users when they interact with disinformation’ (Comm2020) require the use of algorithmic systems to be scalable.

### *Problem outcome*

The future imaginaries of the role of algorithms and their governance in relation to disinformation are rarely addressed directly; yet, it is possible to reconstruct it using priority areas/obligations discussed in the documents. For instance, the Code of Practice (2018) puts special emphasis on the importance of prioritizing relevant, authentic and authoritative information, finding diverse perspectives about topics of public interest, helping consumers understand why they are seeing particular advertisements and improving digital media literacy. The Action Plan (2018) suggests the end result should be the preservation of the democratic process and the trust of citizens in national and EU public institutions. Algorithmic systems should enable at least some of the above-mentioned goals, such as retrieving authentic and authoritative information.

## **Case 2: FinTech**

### *Problem formulation*

The Commission recognizes the financial sector as ‘a major driver in the digital transformation of the economy and society’ (FinAction2018: 2). FinTech is seen as key in



realizing the DSM and Capital Markets Union, increasing the competitiveness of the European financial sector within the global market and enhancing access to financial services and investment for small and medium-sized enterprises (SMEs). On the consumer side, it may 'improve financial inclusion for digitally connected citizens' (FinAction2018: 2). The deployment of algorithmic systems (e.g. big data analytics and AI) are among the key innovations that transform FinTech, while further breakthroughs are expected from blockchain technologies (FinAction2018: 2).

There are several obstacles that impede the uptake of digital innovations in finance. The Commission highlights inconsistencies in how licensing requirements are applied by supervisors of respective Member States; limited interoperability of services, which limits market access to new entrants; uncertainties about compliance requirements when, for example, data processing is outsourced to cloud service providers; and regulatory requirements that are difficult to meet for FinTechs, such as 'requirements or preferences for paper-based disclosures' (FinAction2018: 10).

While the emphasis in the Action Plan lies on how to remove barriers that impede the full realization of FinTech's potential, it acknowledges that the rapid uptake of innovative technologies in the sector also carries with it 'cyber-related risks, data, consumer and investor protection issues and market integrity issues' (FinAction2018: 2). These threats can undermine the financial sector by decreasing confidence and trust on the part of markets and consumers and may lead to the destabilization of markets and undermining of the integrity of the EU financial system.

Compared to policy documents that preceded it, in particular the EP resolution on FinTech (2017) and the FinTech consultation document (2017), the Action Plan (2018) has a more narrowly defined problem formulation. For example, the Parliament also refers to the possible effects of automation in finance on employment and the need for investing in skills (re)training, the risk of discriminatory use of consumer data and negative implications of dynamic pricing for consumers (FinEPres2017). It addresses 'robo-advice' and its assumed contribution to enhancing financial inclusiveness but emphasizes how 'errors or biases in algorithms or in the underlying data can cause systemic risk and harm consumers' (FinEPres2017, 10). The EP thus signalled the importance of protecting consumer rights, including in consumer financial advice, data validity and processing. A significant number of these were included in the consultation document, which acknowledges risks such as data errors and the role of social media and automated matching platforms in crowdsourcing credit (FinConsultation2017). Yet, it presents consumer safety as a financial risk, not as a possible societal harm. These concerns did not make it into the Action Plan, which is noticeably more concerned with the market side, rather than the consumer side of FinTech.

### *Problem solution*

While the EP outlines the various possibilities enabled by FinTech it wants to see realized, the potential risks involved and the criteria future policy should uphold, the solutions it proposes are sketched in more broad strokes (FinEPres2017). The resolution emphasizes the need to review existing regulatory frameworks and enforce the rights and obligations they provide, while simplifying regulatory supervision. For example,

regarding the General Data Protection Regulation (GDPR), the Parliament recalls how the Directive ‘grant[s] the data subject the right to obtain an explanation of a decision reached by automated processing and to challenge this decision’ and how it requires a ‘guarantee that incorrect data can be changed and that only verifiable and relevant data are used’ (FinEPres2017: 9). To address its concern about data errors, biases or discrimination in financial services such as robo-advice, it calls on the Commission to propose a strategy on data sharing ‘with the aim of putting consumers in control of their data’ (FinEPres2017: 9) and for the Commission and European supervisory authorities ‘to monitor these risks’ (FinEPres2017: 10). The consultation document asks whether ‘enhanced oversight of the use of artificial intelligence (and its underpinning algorithmic infrastructure) [is] required and suggests that this may be done through ‘initial and ongoing review’ of this infrastructure, ‘including transparency and reliability of the algorithms’ (FinConsultation2017: 8). It also asks whether there should be minimum requirements for the ‘characteristics and amount of information about the service user and the product portfolio’ included by service providers in, for example, algorithmically generated risk profiling (FinConsultation2017: 8). Regarding the expansion of social media into FinTech and automated matching platforms, it asks whether self-regulation (how the EU typically approaches the regulation of social media platforms) is sufficient.

In the Action Plan, the Commission concludes that only ‘targeted initiatives for the EU to embrace digitalization of the financial sector’ are warranted (FinAction2018: 5). Pointing towards the pace of developments, the Commission positions itself against ‘overly prescriptive and precipitous regulation’ which may have ‘undesired outcomes’, while acknowledging that ‘refraining from updating policy and regulatory frameworks may place EU financial service providers at a disadvantage in an increasingly global market’ (FinAction2018: 17). Beyond reviewing existing regulatory frameworks and promoting interoperability, the Commission proposes establishing regulatory sandboxes, as also suggested by the Parliament (FinEPres2017). This would facilitate greater exchange of information between firms and regulators and ensure supervision can be ‘tailored to innovative firms or services’ (FinAction: 9).

Many of the risks associated with FinTech, the Action Plan (2018) states, are covered by existing regulatory frameworks, including the GDPR; yet the exercise of regulatory oversights should be guaranteed as the role of digital technologies expands. Here, RegTech is singled out as a potential solution for regulatory compliance and supervision. To address cybersecurity vulnerabilities, practicing cyber hygiene is important (FinAction2018: 16). Access to threat intelligence and information sharing are fundamental to improving cybersecurity in finance, as are more active penetration and resilience testing.

In terms of algorithmic solutions, the Action Plan suggests algorithm-enabled, data-driven services could help non-professional individual investors to select suitable investment products. Automated-advisors, online comparison tools and related digital solutions could enhance the distribution of such retail investment products within the *DSM*. While mentioning the algorithms used should be ‘appropriate’ and that results should be ‘presented in a fair and easy to understand way’, no further conditions or safeguards are specified (FinAction2018: 15). Other ways of ensuring that FinTech will contribute to

greater financial inclusion of citizens are not given. Since the issue of TechFins, that is, the expansion of big technology firms into financial services, is not made explicit in the Action Plan, no particular solutions are offered apart from the general aims of facilitating competition.

### *Problem outcome*

The examined documents on FinTech more eagerly engage with visions of the future. Similar to other domains (e.g. smart energy), the FinTech-related interpretations of the future role of technology are predominantly positive. FinTechs are said to bring about ‘incremental innovation and increase[d] efficiency’ in existing markets while creating new markets, thereby making the EU economy more competitive and fostering integration within the DSM (FinConsultation2017: 4). The use of technology ‘can help to deepen and broaden EU capital markets by integrating digitisation to change business models through data-driven solutions’ (FinAction2018: 2). Consequently, FinTech is believed to provide the means for making the European financial sector better able to compete with its global competitors, resulting in ‘a thriving and globally competitive European financial sector that brings benefits to the EU economy and its society’ (FinConsultation2017: 4). The notion that the ‘platformisation’ of FinTech means that its future development is likely characterized by ‘[p]rocesses of [market] consolidation rather than competition’ (Langley and Leyshon, 2021: 382) does not figure in this vision.

### **Conclusion**

The aim of this article was to examine how challenges and risks associated with algorithmic governance are imagined and narrated in the context of EU-level policies. Analysing the conceptualization of the present and future role of algorithmic systems in the context of online disinformation and FinTech, we aimed to contribute towards a greater understanding of the context specificity of how algorithmic governance is understood and uncover the assumptions on which these systems’ evaluation within different domains is based. Our analysis shows that the sociotechnical imaginaries prevalent in policy documents connected to the Action Plan on Disinformation and the FinTech Action Plan are highly divergent. While the first can be characterized as an algorithm-facilitated attempt to return to the presupposed status quo – the absence of manipulation and citizens reliant on authoritative information sources – the latter places technological innovation at the centre of realizing a globally competitive and integrated DSM. These imaginaries are important as they (de)legitimate ways of governing and may create path dependencies. In the case of online disinformation, the sociotechnical imaginary authorizes ‘techno-solutionist’ thinking, while the lack of a long-term vision impedes the full acknowledgement of the importance of alternative approaches, such as nurturing a thriving media ecology. For FinTech, the imaginary authorizes the reinforcement of the ‘platform political economy’ dynamics at play, which may result in the opposite of the intended effect, while the consumer dimension is conveniently placed ‘beyond scope’.

In our analysis, we focused on normative documents produced by the Commission, Council and Parliament and did not include, for example, other European institutions

or industry frameworks and best practices used in the respective sectors. Future research analysing, for example, non-compliance documents coming from the industry, as well as studies into lobbying activities and stakeholder consultations may uncover the characteristics and influence of such institutional, corporate and counter-imaginaries. While beyond the scope of this study, future research may also assess to what extent the future imaginaries formulated in the proposed Digital Markets Act and Digital Services Act, which aim to rebalance the responsibilities of platforms, users, and authorities by establishing a transparency and accountability framework for platforms to better protect customer rights, succeed in overcoming some of the limitations we identified. Finally, it would be advantageous for future studies to supplement document analysis with interviews to investigate how the future of governance-related policies is perceived by policymakers and how they view the long-term effects of these policies.

While it may be tempting to dismiss the identified differences between disinformation and FinTech as being merely the result of the different policy domains that produce them, we propose a different interpretation. First, the treatment of algorithmic governance as a mixed phenomenon in the domain of disinformation – one producing both disruptive and restorative effects to the public sphere – and as a primarily positive one in the case of FinTech can be attributed to the different role algorithmic systems play in the (un)making of power hierarchies. In the former case, transnational governance structures operate from a reactive position, related to the intense use of algorithms for ‘levelling the field’ between categories of actors. Similar to how online platforms have been leveraged to counter power imbalances between state-controlled media and grassroots activists in authoritarian states, the amplification power enabled by algorithms now allows alternative agents to promote their views and interpretations (in this case, not to promote but undermine democracy). By contrast, the deployment of algorithms in FinTech is promoted as part of the EU’s proactive position on facilitating innovation in finance. The emphasis on the realization of the DSM also reflects how FinTech, as a policy issue, is much closer aligned to the EU’s core competencies and those policy domains where it has extensive leverage to act, as compared to governing the legitimate boundaries to online speech.

The difference in maturity level of the policy domains, namely that the financial sector is already subject to extensive EU regulatory oversight, which was strengthened after the 2008 financial crisis, may also play a role. Yet, the assumption, evident from the Action Plan, that existing frameworks concerning personal data and consumer protection sufficiently safeguard against socio-economic effects of automated decision-making in finance (e.g. discrimination when data profiles are used for assessing credit worthiness by online platforms) appears misguided in light of the EU’s efforts to counter discrimination on and by social media platforms who are similarly bound by, for example, the GDPR.

The divergence between the cases also illustrates the ‘crisisification’ of EU policy-making in which there is a ‘determined focus on finding the next urgent event, a prioritization of speed in decision-making, new perceptions of which actors matter, and new narratives on the role and purpose of the EU’ (Rhinard, 2019: 629). Whereas, on FinTech, the policy cycle largely follows the traditional steps (consultation procedure),


the response to the disinformation ‘crisis’ looks very different. While the FinTech documents explicate a clear end point – a sociotechnical future – and steps towards its realization, the disinformation documents focus on calling a halt to the identified danger *now*, without clear guidelines for how digitally mediated information flows can be governed differently to safeguard public discourse in an ever-changing future. EU crisis policymaking often involves technical solutionism in an effort to both act and ‘depoliticize contentious issues’ (Rhinar, 2019). In the case of the disinformation crisis, yet another rapid alert system to this end was indeed established, even though the basic notions on which this system should operate remain contested. The push towards stopping disinformation, in particular with the help of automated approaches, can reinforce censorship and facilitate manipulation by state authorities, in particular in Member States where democratic systems are weak or weakening. The lack of a clearly formulated future perspective means that there are few benchmarks to assess these solutions against and prevent negative impacts on civil rights.

The different temporal horizons and normative assessments identified through our comparative research design demonstrate how this approach is effective for identifying and explaining context specificity in algorithmic governance and helps uncover the assumptions that underlie the evaluation of algorithmic governance within different policy domains.

## Funding

The author(s) received no financial support for the research, authorship and/or publication of this article.

## ORCID iDs

Mariëlle Wijermars  <https://orcid.org/0000-0001-7735-4403>

Mykola Makhortykh  <https://orcid.org/0000-0001-7143-5317>

## References

- Beckert J (2016) *Imagined Futures: Fictional Expectations and Capitalist Dynamics*. Cambridge, MA: Harvard University Press.
- Bellanova R and De Goede M (2022) The algorithmic regulation of security: an infrastructural perspective. *Regulation & Governance* 16: 102–118.
- Bennett Moses L and Chan J (2018) Algorithmic prediction in policing: assumptions, evaluation, and accountability. *Policing and Society* 28(7): 806–822.
- Bennett O (2021) The promise of financial services regulatory theory to address disinformation in content recommender systems. *Internet Policy Review* 10(2): 1–26.
- Bradshaw S (2019) Disinformation optimised: gaming search engine algorithms to amplify junk news. *Internet Policy Review* 8(4): 1–24.
- Brown J (2020) Algorithms and vulnerable citizens: the cost of Australia’s experiment with automation in the governance of its social welfare system. *The Public Sphere: Journal of Public Policy* 8(1).
- Bruns A (2019) *Are Filter Bubbles Real?* Hoboken, NJ: John Wiley & Sons.
- Burri RV (2015) Imaginaries of science and society: framing nanotechnology in Germany and the United States. In: Jasanoff S and Kim H (eds) *Dreamscapes of Modernity: Sociotechnical*

- Imaginaries and the Fabrication of Power*. Chicago, IL: The University of Chicago Press, pp. 233–253.
- Campbell-Verduyn M, Goguen M and Porter T (2017) Big data and algorithmic governance: the case of financial practices. *New Political Economy* 22(2): 219–236.
- Carlson AM (2017) The need for transparency in the age of predictive sentencing algorithms. *Iowa Law Review* 103: 303–329.
- Carstens A (2018) Big tech in finance and new challenges for public policy. Keynote address, FT Banking Summit London, 4 December. Available at: <https://www.bis.org/speeches/sp181205.htm> (accessed 22 December 2020).
- Cœuré B (2018) Financial regulation and innovation: a two-way street. Introductory remarks at a roundtable organised by FinLeap, Berlin, 14 March. Available at: <https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180314.en.html> (accessed 22 December 2020).
- Coglianese C and Lehr D (2019) Transparency and algorithmic governance. *Administrative Law Review* 71: 1–56.
- Danaher J, Hogan MJ, Noone C, et al. (2017) Algorithmic governance: developing a research agenda through the power of collective intelligence. *Big Data & Society* 4(2): 1–21.
- De Goede M (2012) *Speculative Security: The Politics of Pursuing Terrorist Monies*. Minneapolis, MN; London: University of Minnesota Press.
- Di Pietro R, Raponi S, Caprolu M, et al. (2021) *New Dimensions of Information Warfare*. Berlin: Springer.
- Eagle S (2001) *Regulatory Takings*. New York: Lexis Publishing.
- Ferrara E (2017) Disinformation and social bot operations in the run up to the 2017 French presidential election. *First Monday* 22(8).
- Festic N (2022) Same, same, but different! Qualitative evidence on how algorithmic selection applications govern different life domains. *Regulation & Governance* 16: 85–101.
- Gorwa R, Binns R and Katzenbach C (2020) Algorithmic content moderation: technical and political challenges in the automation of platform governance. *Big Data & Society* 7(1): 1–15.
- Graaf SVD (2018) In waze we trust: algorithmic governance of the public sphere. *Media and Communication* 6(4): 153–162.
- Gritsenko D and Wood M (2022) Algorithmic governance: a modes of governance approach. *Regulation & Governance* 16: 45–62.
- Groves C, Henwood K, Shirani F, et al. (2016) The grit in the oyster: using energy biographies to question socio-technical imaginaries of ‘smartness’. *Journal of Responsible Innovation* 3(1): 4–25.
- Gruin J (2019) Financializing authoritarian capitalism: Chinese FinTech and the institutional foundations of algorithmic governance. *Finance and Society* 5(2): 84–104.
- Helberger N (2019) On the democratic role of news recommenders. *Digital Journalism* 7(8): 993–1012.
- Jasanoff S and Kim SH (2009) Containing the atom: sociotechnical imaginaries and nuclear power in the United States and South Korea. *Minerva* 47(2): 119.
- Kalpokas I (2019) *Algorithmic Governance: Politics and Law in the Post-human Era*. Berlin: Springer.
- Katzenbach C and Ulbricht L (2019) Algorithmic governance. *Internet Policy Review* 8(4): 1–18.
- König PD (2020) Dissecting the algorithmic leviathan: on the socio-political anatomy of algorithmic governance. *Philosophy and Technology* 33: 467–485.
- Kucharczyk J (2019) When product innovation becomes competition infringement. Preliminary thoughts on the. *Google Shopping Decision*. *European Competition and Regulatory Law Review* 1(3): 193–197.
- Langley P and Leyshon A (2021) The platform political economy of FinTech: reintermediation, consolidation and capitalisation. *New Political Economy* 26(3): 376–388.



- Larsson S (2018) Algorithmic governance and the need for consumer empowerment in data-driven markets. *Internet Policy Review* 7(2): 1–13.
- Latzer M and Festic N (2019) A guideline for understanding and measuring algorithmic governance in everyday life. *Internet Policy Review* 8(2): 1–19.
- Latzer M, Hollnbuchner K, Just N, et al. (2016) The economics of algorithmic selection on the Internet. In: Bauer J and Latzer M (eds) *Handbook on the Economics of the Internet*. Cheltenham; Northampton, MA: Edward Elgar, pp. 395–425.
- Makhortykh M, Urman A, and Ulloa R (2020) How search engines disseminate information about COVID-19 and why they should do better. *The Harvard Kennedy School Misinformation Review* 1(1): 1–12.
- Mansell R (2014) Here comes the revolution: the European digital agenda. In: Donders K, Pauwels C and Loisen J (eds) *The Palgrave Handbook of European Media Policy*. Basingstoke: Palgrave Macmillan, pp. 202–217.
- Marsden C, Meyer T and Brown I (2020) Platform values and democratic elections: how can the law regulate digital disinformation? *Computer Law & Security Review* 36: 105373.
- Mersch Y (2019) Lending and payment systems in upheaval: the FinTech challenge. In: *Speech at the 3rd annual conference on FinTech and digital innovation*, Brussels, 26 February. Available at: <https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190226~d98d307ad4.en.html> (accessed 22 December 2020).
- McGregor L, Murray D and Ng V (2019) International human rights law as a framework for algorithmic accountability. *International & Comparative Law Quarterly* 68(2): 309–343.
- Mittelstadt B (2016) Automation, algorithms, and politics: auditing for transparency in content personalization systems. *International Journal of Communication* 10: 4991–5002.
- Möller J, Trilling D, Helberger N, et al. (2018) Do not blame it on the algorithm: an empirical assessment of multiple recommender systems and their impact on content diversity. *Information, Communication & Society* 21(7): 959–977.
- Müller-Birn C, Dobusch L and Herbsleb JD (2013) Work-to-rule: the emergence of algorithmic governance in Wikipedia. In: *Proceedings of the 6th international conference on communities and technologies*, June, pp. 80–89. Available at: [https://www.iisi.de/wp-content/uploads/2018/07/ct2013\\_proceedings\\_s3-1\\_mueller\\_dobusch\\_herbsleb.pdf](https://www.iisi.de/wp-content/uploads/2018/07/ct2013_proceedings_s3-1_mueller_dobusch_herbsleb.pdf)
- Napoli PM (2015) Social media and the public interest: governance of news platforms in the realm of individual and algorithmic gatekeepers. *Telecommunications Policy* 39(9): 751–760.
- Noble SU (2018) *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press.
- Olhede S and Rodrigues R (2017) Fairness and transparency in the age of the algorithm. *Significance* 14(2): 8–9.
- Pasquale F (2015) *The Black Box Society*. Cambridge, MA: Harvard University Press.
- Rhinard M (2019) The crisisification of policy-making in the European Union. *Journal of Common Market Studies* 57(3): 616–633.
- Riis T and Schwemer SF (2019) Leaving the European safe harbor, sailing towards algorithmic content regulation. *Journal of Internet Law* 22(7): 1–21.
- Ruppert E (2019) Different data futures: an experiment in citizen data. *Statistical Journal of the IAOS* 35(4): 633–641.
- Sætra HS (2020) A shallow defence of a technocracy of artificial intelligence: examining the political harms of algorithmic governance in the domain of government. *Technology in Society* 62: 101283.
- Saurwein F and Spencer-Smith C (2020) Combating disinformation on social media: multilevel governance and distributed accountability in Europe. *Digital Journalism* 8(6): 820–841.

- Sivarajah U, Kamal MM, Irani Z, et al. (2017) Critical analysis of Big Data challenges and analytical methods. *Journal of Business Research* 70: 263–286.
- Townley C, Morrison E and Yeung K (2017) Big data and personalized price discrimination in EU competition law. *Yearbook of European Law* 36(1): 683–748.
- Van Drunen MZ (2020) The post-editorial control era: how EU media law matches platforms' organisational control with cooperative responsibility. *Journal of Media Law* 12: 166–190.
- Westermeier C (2020) Money is data – the platformization of financial transactions. *Information, Communication & Society* 23(14): 2047–2063.
- Wisser L (2019) Pandora's algorithmic black box: the challenges of using algorithmic risk assessments in sentencing. *American Criminal Law Review* 56: 1811.
- Zetsche DA, Buckley RP, Arner DW, et al. (2018) From FinTech to TechFin: the regulatory challenges of data-driven finance. *New York University Journal of Law & Business* 14(2): 393–446.
- Zilgalvis P (2014) The need for an innovation principle in regulatory impact assessment: the case of finance and innovation in Europe. *Policy & Internet* 6(4): 377–392.

### Author biographies

Mariëlle Wijermars is an Assistant Professor in Cyber-Security and Politics at Maastricht University and a Visiting Researcher at the University of Helsinki. She conducts research on algorithmic governance and the human rights implications of Internet policy. She is co-editor of *The Palgrave Handbook of Digital Russia Studies* (Palgrave Macmillan, 2021) and *Freedom of Expression in Russia's New Mediasphere* (Routledge, 2020).

Mykola Makhortykh is a Postdoctoral Researcher at the Institute of Communication and Media Studies at the University of Bern. His research on, among other subjects, news recommender systems, search engines and digital memory studies has appeared in journals, including *European Journal of Communication*, *Internet Policy Review* and *New Media & Society*.