

Reflections on Algorithmic Governance Responding to AI-Mediated Mobilization and Computational Propaganda Within the Framework of Digital Sovereignty

Xing Zeng

School of Sociology and Social Policy, University of Leeds, LS2 9JT, Leeds, UK

Abstract

In this article, we contextualise the response of algorithmic governance to AI-mediated mobilisation and computational propaganda within the broader frame of digital sovereignty. The study does not focus on technicalities of single systems, but contextualises algorithmic governance in relation to central arguments on code as regulation, surveillance capitalism, digital sovereignty and risk-based AI regulation. It argues that AI-mediated mobilisation and computational propaganda reveal systemic tensions between claims of sovereignty, transnational infrastructures and design-based modes of control, such as hypernudging and *lex algorithmica*. This essay explores how discourses of digital sovereignty, algorithmic risk governance and binding frameworks like the EU AI Act can be read as attempts to regain meaningful control over the algorithmic infrastructures that govern public communication by drawing on conceptual and regulatory literature. The essay argues that good solutions to AI-mediated mobilisation and computational propaganda require multi-layered governance designs that take digital sovereignty as a substantive goal, without resorting to purely defensive or isolationist approaches.

Keywords

Algorithmic governance; digital sovereignty; computational propaganda; AI-mediated mobilization; surveillance capitalism; risk-based regulation.

1. Introduction

The rapid diffusion of artificial intelligence and algorithmic technologies in communication settings has changed the way political messages are produced, distributed and received. Social media feeds, search engines, content recommendation systems and generative models are now influencing what people see, when they see it, and how it is presented. In these cases political mobilisation and propaganda do not need to be human-organized campaigns. They are more and more mediated by computational infrastructures.

At the same time, the topic of digital sovereignty has become a significant problem in many jurisdictions. States, regional organisations and civil society groups are discussing whether and how they can effectively regulate algorithmic infrastructures which are often multinational, privately owned and opaque. Digital sovereignty is presented as a solution to the problem of external dependency, but also of internal accountability problems.

This paper explores the reaction of algorithmic governance to AI-driven mobilisation and computational propaganda within the framework of digital sovereignty. It is normative and philosophical in its bent. The purpose is to consider how different understandings of code as regulation, algorithmic governance, surveillance capitalism and digital sovereignty can be used to address novel forms of AI-led mobilisation and computational propaganda, without relying on proprietary datasets or new quantitative evidence.

2. Digital Sovereignty and Algorithmic Governance

The notion of digital infrastructures challenging sovereignty is a continuation of earlier debates on the regulability of cyberspace. As Lessig says, code is legislation, determining what we may and cannot do online [1]. This concept is relevant to debates on digital sovereignty as it argues that control is exerted not just by formal legal regulations but also by the architecture of systems and protocols.

Digital sovereignty has since become a central theme in policy debates at the European and global level. Digital sovereignty is “the need for more self-determination and decision power on digital infrastructures and technology” [7]. According to Pohle and Thiel, the term is used in relation to state, economic and individual dimensions, with different but overlapping claims to autonomy and control.

Algorithmic governance adds a further element to the situation. This is a kind of regulation-by-design: hypenudges are used to make realtime adjustments to option settings. “Large data-driven decision-guidance systems [4] are described by Yeung as “. Latzer and Festic expand the idea of algorithmic governance to include the steering effects of algorithmic selection systems and the possibility of design-based regulation at a large scale [5]. From the point of view of digital sovereignty, these stories are about governance that is increasingly integrated in the infrastructures of information flows and decision processes.

Such systems are economically and politically important as highlighted by Zuboff’s notion of surveillance capitalism [6]. She argues that the extraction of behavioural data and the construction of predictive models have created new forms of power in which human experience is converted into behavioural excess and fed into predictive and behavioural manipulation systems. This presents concerns from a sovereignty point of view, as to who controls these infrastructures, under whose legal regimes and with what accountability mechanisms.

Digital sovereignty and algorithmic governance offer a conceptual framework to think about AI-mediated mobilisation and computational propaganda . Digital sovereignty is concerned with who should be in meaningful control of algorithmic infrastructures. Algorithmic governance is concerned with how control is exerted on persons and publics through those infrastructures.

3. AI-Mediated Mobilization and Computational Propaganda

Computational propaganda is the use of algorithms, automation, and human curation to purposely distribute false or misleading information to people online [2]. Woolley and Howard observe that bots, fake accounts, and algorithmic amplification are used in combination to sway public opinion across platforms [2]. Their work shows how computer propaganda works by imitating human conduct, by automating repetition and by abusing the features of platforms.

Benkler et al. build on this work by considering the structural vulnerability of media ecologies to feedback loops of propaganda [3]. Their analysis of networked political communication demonstrates how institutional, cultural, and technological factors may combine to create asymmetrical information environments, where some segments of the media environment are particularly vulnerable to manipulation. The architecture of AI-mediated mobilisation is to identify, amplify and coordinate communications, using computational tools.

Yeung’s hypenudging explanation provides a tool for theorising how algorithmic systems mediate mobilisation beyond explicit communication [4]. Hypenudges are also designed to influence behaviour through subtle design-based interventions by dynamically modifying decision settings through ongoing data analysis. Using similar methods for political communication can tell us which topics are significant, which interpretations are prominent, and how folks navigate information spaces.

Latzer and Festic's position on algorithmic governance identifies that algorithmic systems can be intentionally utilised as a mechanism of control but they can also contribute to unintended effects of steering [5]. AI-mediated mobilisation and computational propaganda so encompass not only planned efforts, but also the structural characteristics of platforms and recommendation algorithms which may amplify polarising, or false, material even in the absence of direct orchestration.

Zuboff's analysis of surveillance capitalism demonstrates how infrastructures of ongoing behavioural tracking and prediction enable AI-enabled mobilisation and computational propaganda [6]. There may be optimisation for advertising or engagement inside these systems that can be hijacked or re-purposed for political influence. This convergence makes it hard to discern the line between commercial customisation and political influence.

Digital sovereignty demonstrates that AI-mediated mobilisation and computational propaganda expose gaps in infrastructure control and democratic self-determination. They explain how AI-mediated infrastructures might be exploited by external players, domestic actors or platform owners, to shape public discourse in ways that could escape standard accountability channels. The cures for algorithmic governance should, therefore, be aimed at the design of systems as well as the broader political-economic context within which they operate.

4. Algorithmic Governance Responses Within Digital Sovereignty Frameworks

Some of these concerns are now being addressed through legal and regulatory action. The EU's Artificial Intelligence Act applies a risk-based approach to artificial intelligence systems, prohibiting some high-risk approaches (such as social scoring) and requiring openness, risk management and supervision [8]. The Act is a model of algorithmic governance, with legal criteria for classifying systems by risk level and obligations for suppliers and deployers.

The AI Act is not without peers. European data governance initiatives like the Data Governance Act and related measures aim to provide institutional frameworks for trustworthy data sharing and utilisation [9]. Together, these initiatives attempt to integrate digital sovereignty into the legal and institutional framework by ensuring the consistency of artificial intelligence systems and data practices with fundamental rights, justice and public interest objectives.

According to Pohle and Thiel [7] digital sovereignty can be described as an attempt to recover control over digital infrastructures on a state and regional level. Simultaneously, their work indicates contradictions between the state, economic and private dimensions of sovereignty. So for algorithmic governance digital sovereignty is not one uncontested purpose, but a field of conflicting assertions about who controls what, for whom.

Current AI risk governance models explicitly describe digital sovereignty as a first order objective. The Integrated AI Risk Governance Framework proposes a four-layer paradigm (policy, institutional supervision, technical controls, and operational execution) on categories such as sovereignty-related risk [10]. The idea is that meaningful governance requires a combined control over the legal, organisational and technical domains, by combining data sovereignty, infrastructure sovereignty and decisional autonomy.

At the same time, studies of the sovereignty-internationalism dilemma in AI governance caution that sovereignty claims must be balanced with the need for international cooperation [11]. AI-mediated mobilisation and computational propaganda tend to be international in character, including cross-border infrastructures and actors. Algorithmic governance remedies that are limited to domestic control may be ineffective if they do not account for transnational dependencies and common vulnerabilities.

The findings point to an emergent architecture of algorithmic governance to institutionalise claims to digital sovereignty. Risk-based regulation, governance boards and oversight offices are expected to provide organised control over artificial intelligence systems, especially those that may contribute to manipulative mobilisation and computational propaganda. But they also bring questions regarding the exercise of sovereignty and whose interests are prioritised in the determination of what constitutes legitimate uses of AI-mediated influence.

5. Design-Based Governance, Surveillance Capitalism, and Sovereignty Tensions

Responses to algorithmic governance do not occur in a vacuum. They are combined with the current design based control and economic power. In the hypernudge concept of Yeung and the design-based governance study of Latzer and Festic, behaviour can be steered by algorithmic systems via embedded design, often without the subjects' express understanding [4][5]. This leads to the question to what extent governance solutions based on comparable approaches are capable of reproducing the problems they are supposed to solve.

Zuboff's work on surveillance capitalism puts these issues within the framework of a new logic of accumulation where producing profits requires behavioural surveillance and manipulation [6]. Hence, AI-mediated mobilisation and computational propaganda can be seen as specific cases of a larger regime where algorithmic systems are expected to predict, classify and affect conduct at scale. Regulators need to respond not only to particular campaigns but to the underlying incentives that enable pervasive behavioural instrumentation.

As Lessig argues in *Code is Law* [1], the design decisions made within algorithmic systems can either work against or support these tendencies. Purely openness- or disclosure-based measures of algorithmic control may fall short if they do not modify the underlying systems that enable hypernudging and pervasive surveillance. This notion of digital sovereignty entails a consciousness on the part of the users as to who is designing and directing the code that makes public communication possible.

As discussed in the literature on computational propaganda [2][3], AI-mediated mobilisation is achieved through hybrids of human and automated procedures. And there are specific controls for automated things like bots that don't allow for human organised attempts. Broad limitations, however, risk choking genuine mobilisation and expression. The friction this arrangement causes illustrates the challenge of distinguishing destructive computational propaganda from legal political communication in ways that are consistent with democratic norms.

Studies of digital sovereignty show that sovereignty claims can be used to defend democratic self-determination but also to justify restrictive measures that inhibit open communication [7][11]. The context in which algorithmic governance solutions to AI-mediated mobilisation and computational propaganda are happening is so contentious. They risk sovereignty-based policies being used to centralise informational power in ways that undermine pluralism and accountability.

The concerns underscore the importance of careful design of algorithmic governance within the framework of digital sovereignty, taking into account proportionality, contestability and accountability. It must be against deceptive and opaque practices, but not through excessive surveillance or censorship. Such governance systems may include independent review and public contestation, including design-based technologies such as content labelling, provenance signals and audit logs.

6. Development Directions for Algorithmic Governance

One option is to adopt multi-layered governance frameworks connecting legislative concepts, institutional arrangements, technology standards and operational practices. The Integrated AI Risk Governance Framework provides an example of how digital sovereignty may be operationalised layer by layer, highlighting that governance efficacy is a system attribute and not a function of any one component [10]. This indicates that for AI-mediated mobilising and computational propaganda, such a strategy would be a mixture of regulation, oversight, technical constraints and organisational rules in a coordinated way.

A second approach is to consider sovereignty risks as a distinct category within algorithmic governance. The separation of the frameworks of data sovereignty, infrastructure sovereignty, and decisional autonomy implies that control should be exercised over datasets, technological platforms and decision processes simultaneously [7][10]. This has consequences for AI-mediated mobilisation and computational propaganda including the site of platform hosting, the nature of curation of material and the extent to which domestic authorities have real capacity to monitor and meddle in systems that effect public communication.

Thirdly, transparency and accountability. Algorithmic governance may also support digital sovereignty by controlling disclosure of AI-generated data, registration of system purpose and logging of important decision making [8] [9]. But transparency measures have to be implemented in a way that is clear and accessible for regulators, independent auditors and civil society actors. Otherwise there is a risk that disclosure becomes a box ticking exercise which does not actually boost control or knowledge.

A fourth possibility is to embed contestability in the algorithmic governance frameworks. Where it is impossible to distinguish between legitimate mobilisation and deceptive propaganda, we argue that the legislation should allow for complaints, appeals and public debate on the use of AI-mediated interventions in political communication. This could include civil society oversight structures, access to independent research and procedural safeguards for political actors whose material is affected by algorithmic interventions.

Fifth direction is international cooperation. AI-mediated mobilisation and computational propaganda are threats to cross-border infrastructures and to regulatory inequity. Studies on the problem of sovereignty vs internationalism have indicated that the need for national or regional digital sovereignty must be balanced by collaboration organisations addressing common dangers [11]. Ignoring this factor in measures of algorithmic governance risks rendering them worthless or harmful.

And finally, development initiatives should not reduce the idea of digital sovereignty to a defensive one. Protecting autonomy and removing dependency are not the only elements that characterise digital sovereignty, although they are essential. The power to create digital infrastructures for democratic, social and ethical purposes can also characterise digital sovereignty [7][10]. Algorithmic governance that aims to just reduce external influence will kill the development of desired types of AI-mediated public communication, such as trustworthy information infrastructures and participatory decision support systems.

7. Conclusion

Discussions surrounding AI-mediated mobilisation and computational propaganda highlight the ubiquity of algorithmic systems in public communication and political life. They indicate also that digital sovereignty is necessary for the solutions of problems of control, responsibility and self-determination in the digital.

The paper suggests that algorithmic governance provides a viable yet controversial way to address these concerns. It must resolve tensions between control by design and democratic

accountability, between claims to sovereignty and international interdependence, and between protection from manipulation and preservation of a free political fight.

Algorithmic governance, therefore, should be implemented through multi-layered, sovereignty-aware and contestable arrangements under the umbrella of digital sovereignty. This is not to say that simple solutions will be forthcoming. But it does provide a more realistic basis for addressing AI-mediated mobilisation and computational propaganda in ways that respect both autonomy and pluralism.

References

- [1] Lessig, L. (1999). Code and other laws of cyberspace. Basic Books.
- [2] Woolley, S. C., & Howard, P. N. (2017). Computational propaganda worldwide: Executive summary. Computational Propaganda Project, Oxford Internet Institute.
- [3] Benkler, Y., Faris, R., & Roberts, H. (2018). Network propaganda: Manipulation, disinformation, and radicalization in American politics. Oxford University Press.
- [4] Yeung, K. (2017). 'Hypernudge': Big data as a mode of regulation by design. *Information, Communication & Society*, 20(1), 118–136.
- [5] Latzer, M., & Festic, N. (2019). A guideline for understanding and measuring algorithmic governance in everyday life. *Internet Policy Review*, 8(2). <https://doi.org/10.14763/2019.2.1415>
- [6] Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.
- [7] Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4).
- [8] European Parliament. (2024). Artificial Intelligence Act: Legislative resolution of 13 March 2024 on the proposal for a regulation laying down harmonised rules on artificial intelligence.
- [9] Graux, H., Garstka, K., Murali, N., Cave, J., Botterman, M., & Pellegrin, J. (2025). Interplay between the AI Act and the EU digital legislative framework. European Parliament. <https://doi.org/10.2861/4863883>
- [10] Odion, S., & Addula, S. R. (2026). AI risk governance for advancing digital sovereignty in data driven systems: An integrated multi layer framework. *Future Internet*, 18(4), 209. <https://doi.org/10.3390/fi18040209>
- [11] Ishkhanyan, A. (2025). The sovereignty internationalism paradox in AI governance: Digital federalism and global algorithmic control. *Discover Artificial Intelligence*, 5, 123. <https://doi.org/10.1007/s44163-025-00374-x>