cogitatio

ARTICLE

Reversing the Privatisation of the Public Sphere: Democratic Alternatives to the EU's Regulation of Disinformation

Alvaro Oleart [1] and **Julia Rone** [2]

[1] Department of Political Science, Université Libre de Bruxelles, Belgium
[2] Department of Political Science and Public Administration, Vrije Universiteit Amsterdam, The Netherlands

Correspondence: Julia Rone (j.e.rone@vu.nl)

Abstract

The emergence of social media companies, and the spread of disinformation as a result of their "surveillance capitalist" business model, has opened wide political and regulatory debates across the globe. The EU has often positioned itself as a normative leader and standard-setter, and has increasingly attempted to assert its sovereignty in relation to social media platforms. In the first part of this article, we argue that the EU has achieved neither sovereignty nor normative leadership: Existing regulations on disinformation in fact have missed the mark since they fail to challenge social media companies' business models and address the underlying causes of disinformation. This has been the result of the EU increasingly "outsourcing" regulation of disinformation to corporate platforms. If disinformation is not simply a "bug" in the system, but a feature of profit-driven platforms, public–private cooperation emerges as part of the problem rather than a solution. In the second part, we outline a set of priorities to imagine alternatives to current social media monopolies and discuss what could be the EU's role in fostering them. We argue that alternatives ought to be built decolonially and across the stack, and that the democratisation of technology cannot operate in isolation from a wider socialist political transformation of the EU and beyond.

Keywords

Big Tech; democracy; digital technology; disinformation; European Union; public sphere; social media

1. Introduction: Disinformation as a Feature (not a Bug) of Social Media Platforms

The emergence of social media platforms such as Facebook, Twitter (now X), or TikTok during the last decades has opened a wide political and regulatory debate about the role that these companies play in the

public sphere, and democracy more broadly. The internet and tech platforms are key mediators in the current circulation of ideas and provide the digital infrastructure of modern communication. As Bohman (2004, p. 133) predicted, the mediation of technology in public communication is "an essential condition for the existence of a public sphere in large and highly differentiated modern societies." However, Big Tech social media platforms are not "neutral" spaces through which communication flows circulate, but rather act as gatekeepers, making some actors and ideas more visible than others (Gillespie, 2018). This has become blatantly evident in Elon Musk's use of X, which he bought in 2022 and has since been used to boost Donald Trump's presidential campaign, becoming one of its most visible supporters. In 2024, we saw also open confrontations between X and the Brazilian government: After X refused to name legal representatives in Brazil and to remove profiles associated with disinformation and spreading hate speech, the Brazilian supreme court suspended the social media's service in the country. Brazil's president Lula da Silva famously argued that the world "isn't obliged to put up with [Elon] Musk's far-right free-for-all just because he is rich" (Phillips, 2024).

In the EU context, there have been major concerns around social media platforms' infringement on data privacy, microtargeting in the context of elections, and the spread of disinformation and misinformation. While there is a difference between disinformation (intentionally spreading false information meant to deceive) and misinformation (unintentionally spreading false information), in this article we stick to the concept of disinformation, often used as an umbrella term in EU documents. In fact, countering disinformation has become a central component of the EU's conception of democracy (Oleart & Theuns, 2023) and its strategy of "defending democracy." It is crucial to emphasize that both disinformation and misinformation are connected by being defining features of the business model behind social media platforms such as X or Meta's Facebook. Social media platforms nourish users with the information that is most likely to grab their attention (Benn & Lazar, 2022), regardless of its accuracy, which leads to a loss in the epistemic quality of public deliberation (Chambers, 2021). Scandalous untrue ideas are much better at attracting users' attention, prolonging their time on the platform, and extracting more data from them that can then be used to create profiles that are then sold to advertisers (Borgesius et al., 2018). Disinformation is thus not a bug but a central feature of the business model of tech companies. Indeed, we share Shoshana Zuboff's understanding of tech companies' business model as one rooted in "surveillance capitalism," a logic that is oriented towards mass data extractivism, claiming "human experience as free raw material for translation into behavioural data" (Zuboff, 2019, p. 8).

Rather than addressing Big Tech in general, in this article we focus primarily on social media platforms such as Meta (which encompasses Instagram, Facebook, and Whatsapp), X, Google (which owns Youtube), and TikTok, which have profound consequences for shaping the debates in the public sphere. Indeed, the rise of far-right parties and increasing polarization in contemporary politics are inherently linked to the "disruption" and transformation of the public spheres resulting from the business models of current social media monopolists (Bennett & Pfetsch, 2018; Hoffman & Rone, 2024). What is more, disinformation influences a wide range of other policies, such as health policy and climate change, and thus its regulation emerges as a meta-issue that has an impact on a wide variety of fields.

Considering the high stakes involved it is not a surprise that there has been a wide array of literature oriented to analysing the efforts by public authorities to regulate Big Tech companies (Moore & Tambini, 2021; Simons & Ghosh, 2020). However, most of this literature focuses on the US context and the

possibilities for regulation within its legal landscape—a logical trend considering that most leading social media platforms on a global scale, with the exception of the Chinese TikTok, are US corporations. At the same time, other countries also grapple with the problems of online surveillance and content moderation posed by the ascent of US tech giants. This article focuses more specifically on the agency of the EU in terms of regulating disinformation—a particularly interesting process given the entrepreneurship of the European Commission in this regard and the recent pivot to digital sovereignty (Bonnamy & Perarnaud, 2023; Rone, 2023; Seidl & Schmitz, 2023), but also the EU's broader ambitions to be a global normative leader when it comes to digital regulation (Bradford, 2020; Wagnsson & Hellman, 2018). While the notion of normative leadership has already been problematized in other fields (Staeger, 2016), even the most often quoted success in EU tech regulation and data protection—the General Data Protection Regulation (GDPR)—has so far yielded underwhelming results (Cobbe & Singh, 2022).

In the first part of this article, we argue that the EU has achieved neither digital sovereignty nor normative leadership in regulating disinformation since it has in fact increasingly "outsourced" the regulation of disinformation to corporate platforms. But if disinformation is not simply a "bug" in the system, but a feature of profit-driven platforms, public–private cooperation emerges as part of the problem rather than a solution. We show that the EU is not investing in fostering democratic social media alternatives as part of its new turn to industrial policy. In the second part of the article, we bridge our criticism of current EU policies with the booming field of imagining alternatives to current social media monopolies, outlining six conditions that alternatives to current social media monopolies should satisfy. Finally, we explore what could be the EU's role in fostering such alternatives and point towards hopeful avenues for academic research and political action.

2. The EU's Business-Friendly Regulatory Approach to Disinformation

2.1. Why is the EU Regulating Disinformation?

We could expect assertive action by the EU in the field of regulating disinformation due to the rise of a doctrine of digital sovereignty (Hoeffler & Mérand, 2024; Seidl & Schmitz, 2023), also as the result of concerns about mass surveillance (Bauman et al., 2014) and election interference, but also the increasingly tense geopolitical situation with wars in Ukraine and Palestine, and a rising far right. The concept of digital sovereignty has been applied to a variety of digital fields—including content regulation, AI policy, or semiconductor chips. At the content regulation level, this turn has been expressed in an increasing prioritisation of "public order" over "free access" in discourse (Flonk et al., 2024). And we have seen an assertion of sovereignty also in the ways in which sanctions against Russian media have been imposed throughout the EU, albeit in an uneven and often non-transparent way (ten Oever et al., 2024). The connection between disinformation and sovereignty (Kachelmann & Reiners, 2023) has paved the way for making sense of tech policy as a matter of geopolitics rather than corporate power.

Despite this growing prominence of sovereignty discourses, we argue that the EU's approach to regulating disinformation—both in terms of regulation and investment policy—has failed in challenging the power of aspiring Big Tech corporate sovereigns (Lehdonvirta, 2022; Srivastava, 2022). While the importance of business ideational power and the cooptation of EU institutions have been emphasized in other fields of digital sovereignty pursuit, including cloud policy (Obendiek & Seidl, 2023) or AI policy (Mügge, 2024), less

attention has been drawn to it in the field of disinformation (with important exceptions such as Bouza García & Oleart, 2024; Kausche & Weiss, 2024; Rone, 2021). This is precisely what we aim to do.

Furthermore, the EU has increasingly presented itself as a global normative leader when it comes to digital regulation. In the field of data protection, numerous authors have drawn attention to the de facto and de jure effects of the GDPR in setting global standards and positioning the EU as a normative leader. The regulatory power of the so-called "Brussels effect" (Bradford, 2020) also explains the extent to which lobbying efforts by tech companies have been oriented towards the EU level as a key political space in which we see unfolding the dispute to regulate disinformation, and social media platforms more broadly (Gorwa, 2021; Gorwa et al., 2024). Still, even when it comes to the GDPR as a most prominent success, critical legal scholars have raised doubts regarding the extent to which the regulation actually works and have cautioned against simply replicating more novel regulatory instruments rather than contextualizing them (Ilori, 2022).

An important caveat is needed here: Several authors have argued that the goals of digital sovereignty and normative power are not necessarily aligned and might be even contradictory (Broeders et al., 2023; Wagnsson & Hellman, 2018), due to tensions between discourses of geopolitical leadership and impartial universality. Furthermore, it is not necessarily desirable that the EU becomes a "leader" in the field of digital regulation, as this might reinforce colonial dynamics rather than challenge them. Instead, we focus on why the EU's regulations have missed the mark of addressing the structural causes of disinformation—the corporate-led business models of social media companies—and have simply focused on the symptoms.

2.2. Regulations That Miss the Mark: Tackling the Symptoms Rather Than the Causes

In the last decade, the EU has engaged in a flurry of legislative projects to regulate different aspects of social media companies' operations, including regulations and acts such as the GDPR, the Digital Markets Act (DMA), and the Digital Services Act (DSA). The DMA, applicable for most parts since May 2023, has established a set of clearly defined and objective criteria to qualify certain large online platforms as gatekeepers and to ensure that they behave in a fair way online and leave room for contestability. The DSA, directly applicable across the EU since February 2024, has obliged gatekeeper companies to adopt measures to counter the spreading of illegal goods, services, and content online, as well as to provide greater transparency on content moderation and options to appeal, and to give users more control over the personalization of content (European Commission, 2023).

While it is still unclear what the DMA and DSA's empirical effects or global repercussions will be, it seems they have raised doubts from the beginning. An excellent systematic analysis of the EU's regulatory efforts on disinformation more specifically (Nannini et al., 2024) has shown that problems that were already present in previous EU efforts at regulating tech companies (such as the 2000's E-Commerce Directive or the 2022 code of practice on disinformation), including the limited liability of social media platforms, have in many cases persisted in the novel DSA act. The authors provide a systematization of existing criticism, from a legal and technical perspective (concerns about conceptual ambiguities over what "systemic risk" amounts to), from a behavioural and psychological perspective (the excessive reliance on post-hoc take down measures despite evidence that preemptive friction nudges might be better in containing the spread of disinformation), and finally, from an ethical and philosophical perspective (drawing attention to the dangers of private governance and the outsourcing of truth judgements, the individualized understanding of harm from viral messages, and

the lack of direct journalistic protections). Furthermore, Leerssen (2023) has shown how the DSA aims to end shadow banning by making content moderation more transparent, but this regulation of "demotion" practices is unable to neutralise the structural ranking that social media algorithms undertake when curating content. Interestingly, Meta announced the abandonment of third-party fact-checking, at least in the US, in a gesture of political alignment with the second Trump administration. It remains to be seen whether this will impact its services in the EU (Graves, 2025) and whether other social media platforms will follow, but this would imply a violation of the EU's Code of Practice on Disinformation.

Taking stock of these detailed criticisms, we want to go further and argue that the underlying reason why the new DMA and DSA fail to reassert the EU's sovereignty over content and provide an example of good standard setting on disinformation is that the EU has failed to tackle the very business model of social media platforms, which is one of the root causes for the spreading of disinformation. Currently, the EU seems to see social media platforms as the location of a "marketplace of ideas," a perspective that is compatible with a continuation of reliance on already dominant private companies that "sell" access to "ideas" to their "clients" (users). Arguably, current digital infrastructures perform the "marketplace of ideas" rather successfully—albeit the ideas that are "sold" tend to be those that are most profitable or ideologically desirable for social media companies.

Indeed, the EU's approach has been cautious towards private companies such as Meta or X. A convincing legal and normative analysis of the EU's approach to social media governance by Griffin (2023, p. 58) has illustrated how the EU has deployed a combination of "multistakeholderism" and "rule of law" responses, reinforcing "the image of platforms as benevolent stewards of the public interest, rather than companies pursuing private gain" (Griffin, 2023, p. 60). Pickard (2020, p. 131) likens tech moguls such as Mark Zuckerberg to media barons such as Rupert Murdoch, arguing that a "new social contract for digital media must assert public control over communication systems and provide funding for the public infrastructure that sustains democratic society." In failing to recognise this, the EU's approach is marked by an epistemic and regulatory capture (Farrand, 2014; Obendiek & Seidl, 2023) that systematically sidelines policy demands that may challenge the "surveillance capitalist" business model of social media platforms. In some ways, the EU appears to make sense of Big Tech in a similar way as the big banks after the 2008 financial crash: they are "too big to fail," and policy-makers fail to see the possibility of democratic alternatives.

Regulators in the EU seem to assume that they cannot regulate "against" platforms but should do it "with" them. As a result, when it comes to disinformation, the EU has continuously externalized its regulatory role to platforms. In their endeavour to protect their business model, social media companies have played a crucial role in shaping how to define disinformation policies at the EU level, undermining any strong interpretation of European sovereignty in the field. Thus, EU regulation has ended up with technocratic regulatory changes, for instance, oriented towards algorithmic transparency in the case of the DSA but no substantive changes addressing the root causes of the problem. It is thus a form of detailed, well-intentioned but fundamentally misguided regulation that misses the mark and tackles the symptoms rather than the causes. Current discussions surrounding "disinformation" focus on the regulatory nitty-gritty, while missing the broader and deeper problem that the current infrastructure of the public sphere is reliant on private (global) companies. Furthermore, even if the DMA appears to be less friendly to Big Tech (Hoeffler & Mérand, 2024), competition policy does little to dismantle surveillance capitalism and the data extractivist practices that make targeted advertising and disinformation possible on a mass scale, and a key feature of current public spheres. Even such breaking up would be less than sufficient: Zuboff (2019, p. 23) has

convincingly argued that "calls to break up Google or Facebook on monopoly grounds could easily result in establishing multiple surveillance capitalist firms."

2.3. Why Has the EU Taken Such a Business-Friendly Stand in Regulating Disinformation?

First of all, several key aspects of the current disinformation legislation predate the rise of social media platforms. Limited platform liability was a key principle of legislation already since the late 1990s and early 2000s and it has been invoked multiple times also in progressive mobilizations against surveillance online as seen in the mobilizations against the Anti-Counterfeiting Trade Agreement, in which civil society often sided with Silicon Valley (Rone, 2020).

Secondly, social media companies cooperate closely with policy-makers to shape legislation, preempting public policies that question their business model, while also using their communicative power to challenge political actions that undermine their dominant position (Popiel, 2018). While their reputation has taken a hit, their revenues have continued to increase and social media platforms have emerged as powerful political players in the EU regulatory sphere thanks to their extensive resources. In fact, Big Tech has become "the biggest lobby sector in the EU by spending, ahead of pharma, fossil fuels, finance, and chemicals" (Corporate Europe Observatory, 2021, p. 6).

Third, a major reason for the EU's light-touch business-friendly approach to disinformation lies in the very essence of what is being regulated. Unlike data privacy regulation, which stems from fundamental human rights, regulating disinformation in the EU has a more problematic legal basis, since disinformation, even if harmful, is not illegal per se (Rone, 2021). To be sure, the argument about disinformation's specific legal status should be taken with a grain of salt, since it fails to explain why we have seen many similar developments and regulatory capture also in other digital policy fields such as data privacy, AI, or even cloud policy (Hladikova, 2024; Obendiek & Seidl, 2023). Indeed, a key effort put forward by Big Tech actors is to demonstrate to public authorities that they are indispensable for the regulation of the digital across the stack. For years these companies have dominated the networks of "expertise" at the EU level (Farrand, 2014), and policy-makers have largely relied on their "knowledge" to regulate them.

Finally, social media platforms have been skilful in navigating the series of international crises, managing to reframe a public policy issue such as the regulation of Big Tech as a "geopolitical" issue (Bradford, 2023) that is mostly looked through the lens of "security" (Mügge, 2023; see also Proto et al., 2025). The security-focused and geopolitical framing of disinformation places a great emphasis on the role of foreign actors in spreading disinformation while ignoring the key role of domestic, often far-right actors in creating and sharing disinformation (Rone, 2019). The right-wing framing of "security" and "foreign interference"—mostly referring to China, Russia, or Iran—when conceiving the interaction between tech platforms and democracy has also led EU public authorities to mostly invest human resources in the European External Action Service and the East Stratcom unit, oriented towards fighting disinformation and "foreign interference," while sidelining the role of social media platforms' business model in fostering disinformation (Tuñón Navarro et al., 2019). Given the lower amount of resources of the Directorate-General Connect and other relevant directorate-generals in the European Commission focused on regulating platforms, partially externalising the regulatory role to platforms (e.g., by allowing them to co-draft the code of practice on disinformation) appears also as a pragmatic decision from their perspective. It follows from

this thinking that EU policymakers tend to see social media companies not as part of the problem, but as the solution. However, what if the exact opposite is true: What if public–private cooperation with Big Tech is not part of the solution but instead part of the problem?

2.4. The EU's Lack of Investment in Alternatives

There is a notable lack of ambition by the EU to invest in and foster meaningful alternatives to current social media. When it comes to the cloud, the EU has increasingly combined regulation with targeted investment including through the so-called Important Projects of Common European Interest (Sheikh, 2022). To the contrary, there have been no comparable investment initiatives at the applications layer, relevant for the disinformation problem but also for data privacy, the integrity of elections, and democratic quality overall. Indeed, there have been only a few examples of venture projects to create alternatives to existing platforms such as Facebook, X, or TikTok. Among the few existing examples have been the platforms EU voice and EU video, launched by the European Data Protection Supervisor in 2022, which however have been used mainly by EU institutions so far. Still, (fostering) investment in social media alternatives accessible to the public has been negligible.

This became particularly clear during the first mass exodus from X (formerly Twitter) just after it was bought by Elon Musk in 2022. Back then, the European Commission launched its presence on the bottom-up alternative platform Mastodon, maintained by the German non-profit Mastodon. While Mastodon had received support through the Next Generation Internet programme by the European Commission (funding meant to foster the development of open-source software), in July 2024 it came out that the EU Commission is planning to close this line of funding without any explanation (Henning, 2024). In response, in August 2024, Mastodon's CEO and CTOs published an open letter to encourage the European Commission to continue funding open-source software (Rochko & Chaput, 2024). The fact that the Commission would discontinue its open-source software funding programme and replace it with a programme with less funds and more bureaucracy exactly when most of the world is looking for alternatives to Musk's X is puzzling, to say the least.

A potential reason for this lack of appetite to develop social media alternatives might be precisely the market orientation of EU institutions and its scepticism towards genuinely innovative open-source federated and more democratic alternatives. Indeed, from such a market perspective, the EU has felt that it has lost the competition for consumer data, where US and Chinese social media platforms are dominant, and has focused instead on developing cloud infrastructure for industrial data, where it still has potential (European Commission, 2020). Still, there are reasons to not simply regulate social media platforms but also to search for alternatives that go beyond the economic potential of such investments, including the protection of democracy and the promotion of an inclusive, democratic, and safe public sphere.

3. Towards an Emancipatory, Decolonial, and Democratic Digital Horizon: People's Power Through the Stack

We have so far described the EU's market-based approach to regulating disinformation and the lack of investment in alternatives to Big Tech social media platforms. Here, we bridge this analysis with the burgeoning literature on alternatives to corporate social media, which however has rarely focused on the EU as a policy space. We ask: How can we imagine and build an alternative public infrastructure in a way that is

more democratic and serves a collective purpose rather than the interests of private multinational corporations? This question has raised considerable attention over the last few years (Fuchs, 2021; Grohmann, 2023; Pickard, 2020; Rikap et al., 2024; Muldoon, 2022a, 2022b; Verdegem, 2022). Complementing this literature and applying it to the EU policy space, we argue that rather than a one-size-fits-all alternative to corporate social media monopolists such as Facebook and X, there should be multiple alternatives following six basic principles: (a) a commitment to secure a space for public communication oriented towards the public good rather than profit; (b) a democratic decision-making process surrounding the design and governance of alternatives; (c) plurality (c1) and interoperability (c2) across alternatives; (d) searching for alternatives across the technological stack; (e) non-exploitative and transparent content moderation; and (f) sustainable public funding that makes this possible and contributes to reversing structural inequalities.

Tech companies have managed to achieve an unprecedented feat—to enclose a large part of our communicative space and inter-subjective being on their own private platforms, extracting data for the purposes of their own private profit. Reclaiming "the space of our world" (Couldry, 2024) necessarily involves a rethinking and rebuilding of our common space in ways that cater for the public good rather than for the interests of a few corporations (a). If our digital public sphere can be currently compared to a shopping mall on whose premises we are allowed under the conditions of the owners and with the explicit purpose to be geared towards shops, a real alternative would constitute publicly owned or held-in-commons spaces that are also democratically managed and where we collectively decide what disinformation is and how algorithms should be used to shape conversations (if at all). Relatedly, alternatives should ideally be built on free and open-source code so that there is transparency regarding the software choices made, and the possibility of changing them. Public or community ownership of social media platforms is an even more reasonable suggestion once we acknowledge that a substantial share of the basic technology that makes possible their functioning was developed with public money, while the profit was subsequently privatized (Mazzucato, 2019).

Of course, the question is not simply about who has invested in the technologies that make social media possible and who is reaping the profits. Had this been the case, many of the current problems could have been addressed by redistributing the benefits of "surveillance capitalism," as suggested by Jason Lanier's (2014) proposal to pay consumers for the data collected by Big Tech companies. However, the problem is rather the non-democratic surveillance capitalist business model as such, and the current public spheres' reliance on private companies. Relatedly, the idea of building "European tech champions" has grown during the last few years to reduce the EU's dependence on US tech companies. However, a European version of US Big Tech companies is unlikely to make a meaningful difference if the ownership is in private hands, the business model remains the same, and there is no democratic governance.

Indeed, a democratic decision-making process (b) on what types of alternatives to current social media we would like to achieve would involve elected representatives at multiple levels. But it should also involve inputs from social movements and experimental tech collectives operating outside of the institutional sphere (Levi, 2022). Such actors should also be acknowledged by integrating expertise from below in debates about alternatives to current social media. The articulation of relations of transnational solidarities (Oleart, 2023) and collective action needs to be at the centre of any attempt to democratise alternative digital infrastructure. Widespread media coverage would also be crucial to keep citizens informed and ensure the quality of democratic participation in the design and governance of alternative social media.

Such a democratic approach to governance would be in stark contrast with the arbitrary, almost monarchical approach to governing social media that we see from Musk's X or from Zuckerberg's Meta, where an oversight board has been established with a restricted scope of action, providing no democratic legitimacy to platform governance (Haggart & Keller, 2021), and thus making a mockery of democracy. Considering that Big Tech companies are based in the Global North, a decolonial logic (Couldry & Mejias, 2023) of integrating and empowering collective actors and movements from the Global South should be central to any democratic attempt to develop alternatives.

When thinking of transforming the digital sphere, we need to think of ways in which this transformation could facilitate mass transnational collective action and participation at a local, national, and transnational scale (Oleart, 2021). The challenge is that the democratisation of the public sphere is both a normative goal as well as a necessary precondition for achieving it. This is because activists and political actors that organise against the existing capitalist model need digital spaces for both internal and external communication. On one hand, they need those spaces to effectively organise internally and transnationally, but they also need them to communicate beyond activist spaces (Castells, 2012). Insofar digital spaces are controlled by corporate actors, it is the latter that have the "sovereignty" to close those spaces. There are already several examples in which social media companies have cooperated with authoritarian governments to reinforce racism, violence, and restrict independent reporting (for the case of Myanmar, see Fink, 2018), thus complicating activists' capacity to organise.

Alternative social media platforms, following Muldoon's (2022a) ground-breaking work on platform socialism, could be conceived on different levels (c1)—local, national, and transnational depending on the types of publics they cater for and the types of goals they set themselves. A plurality of existing alternatives that operate simultaneously allows us to avoid thorny questions such as state censorship, for example. In some countries, a national social media, funded by taxpayers' money and democratically governed by its employees under oversight by parliament, for example, could work. In other contexts, where governments have shown authoritarian tendencies and might use social networking platforms for surveillance, bottom-up decentralized networks could be developed or solutions from abroad could be offered. Local social networking platforms could be very useful in terms of finding help for everyday tasks or maintaining neighbourhood life (Lomax-Reese & Wood-Lewis, 2021). But maintaining transnational connections is also crucial in some contexts such as transnational social movements' mobilization. Such connections could be made possible by the existence of transnational social networking platforms governed by bodies such as the UN, for example, where activists could debate and exchange information.

Crucially, using different alternatives to social media should not presuppose absolute loyalty by users to one social media only. It is thus important to create opportunities for users that are compatible and complementary (c2). Users should be able to bring their data from one platform to another, the so-called data portability. Interoperability between different platforms should be encouraged (Doctorow & Keller, 2021) to avoid a lock-in effect, whereby the cost of leaving a platform outweighs the benefits of joining an alternative. Mechanisms could also be developed so that content on one platform can "migrate" to other platforms and be discoverable across platforms. Thus, rather than thinking that the alternative to Instagram, TikTok, or X should be one global platform with equally ambitious goals of "connecting the world," a better pathway forward might be to connect multiple different but interoperable platforms across the globe, each with its own democratic governance bodies. On such a federated network of platforms, disinformation

would not scale up as quickly as on Facebook or X, but would have multiple barriers and thresholds to cross, ultimately receiving less attention.

Furthermore, a lot of existing proposals for alternatives can be enriched by a productive dialogue with critical media and environmental media studies, where the materiality of data has become increasingly emphasized and problematized. The functioning of current social media platforms such as Facebook, X, or TikTok is made possible by the constant work of vast amounts of servers hosted in gigantic data centres across the globe which have considerable energy and water demands (Hogan & Vonderau, 2019; Rone, 2023). Unlike previous public spheres which operated on the agora, on market squares, or in cafes, the digital public sphere is physically hosted on servers. And unlike built environments which require maintenance every now and then, the digital public sphere needs constant material maintenance and access to stable and trustworthy electricity grids.

Borrowing from Benjamin Bratton's speculative notion of the "stack," Haroon Sheikh (2022) outlines seven layers of digital sovereignty, including resources (raw minerals), chips, networks, cloud, intelligence, applications, and connected devices. Thus, any alternatives to the current social media platforms will have to consider power through the stack and to be thought through various layers (d). Conceiving viable alternatives to current social media platforms should not overlook thorny issues such as raw material extraction, network maintenance, and cloud governance—all layers of the stack that come with key trade-offs and challenges (Rikap et al., 2024). In locations where electricity supply is less trustworthy, more decentralized forms of networking and storing data on users' devices thus might be better options than national systems running on centralized servers. In the EU, there have been recent calls for developing a "EuroStack" (Bria et al., 2025), an interesting proposal that nonetheless prioritizes the "competitiveness" and "innovation" of European companies and the "strategic autonomy" of the EU, rather than the democratic and decolonial logic discussed earlier and continues to rely on private–public partnerships.

When thinking about national and transnational platforms, decisions on where and how data centres will be built should be open to democratic discussion, especially considering the heavy environmental consequences and energy demands of data storage. Another crucial question is what data should be stored in data centres and for how long. In the current ad-driven business model of social media companies, all user data is stored and used to improve targeted ads. But in a situation in which platforms are not profit-pursuing entities, collecting and storing all user data in a centralized way would not be necessary. An additional consideration is whether users' data should be used for training AI or not (the "intelligence layer"). Decisions on this matter would depend a lot on who manages the platforms, for what purposes, and what the purpose of training AI would be. In a world where multiple interoperable social media platforms exist, the decision of what data to store, for how long and how it would be used might differ per platform and context.

Fifth, while all previous principles are relevant for solving not only disinformation-related problems but also all kinds of other issues (data privacy, surveillance, expropriation of the commons...), an issue of great importance specifically for the topic of disinformation, is who will perform the content moderation labour on alternative social media platforms. Currently, this work is often externalized by the platforms and outsourced to workers under poor conditions—often in the Global South—who expose themselves to psychologically traumatizing content for small remuneration (Muldoon et al., 2024; Parks, 2019). Believing that a democratically designed and governed social media platform would not need moderation is naïve. The question emerges: Who will

do the moderation and under what labour conditions? Also, how will it be decided what content counts as disinformation? A non-exploitative and transparent moderation system should be pursued, in which securing transparent and democratically agreed criteria on content moderation and shielding moderators from harm (e) are the norm.

Finally and fundamentally, we must address the question of who would fund the initial prototyping and development of alternatives to current social media (f). This could happen through targeted public funding and investment—the sort of which is currently missing at the EU level when it comes to the applications layer. It could also happen through national government and municipal funding for smaller-scale projects. Not-for-profit charity funding could also be the basis of the initial development of alternative projects. Once built, social media platforms that are liked and adopted by users could be funded by taxpayers' money (see Crum, 2023, on the BBC as a reference case) or through membership and subscription fees. Indeed, the subscription model has been recently proposed by Facebook itself to users in Europe. The problem with Facebook's offer though is that users who pay for subscriptions, supposedly, would not have their data shared with advertisers. What this means in effect is that those who do not pay will have their data shared, introducing a crude distinction between those able to pay and those who are not. Data extractivism is something we have observed happening on a large scale when it comes to citizens' data in Africa (Kalema, 2023), and it has been a crucial element of digital or data colonialism (Couldry & Mejias, 2019; Kwet, 2019; Lehuedé, 2023).

Whatever alternative forms of funding social media platforms citizens, governments, and social movements come up with, these forms should not lead to a digital apartheid between those who can afford to not have their data collected and those whose data is mined and used for developing AI, reinforcing structural injustices in society. Rather than reproducing capitalist and colonial logics, new forms of funding should thus be based on innovative models that foster bonds of solidarity, meaning that (a) those who can afford could and should pay for access to the digital public sphere of those who cannot afford it, and (b) data extractivism should be eliminated rather than curtailed through pay-out options for those who can afford it. This requires a global approach that is sensitive to the structural inequalities and exploitation within and between the Global North, the Global South, and the Global East.

Our main point is that combatting disinformation is just one aspect of the broader task of democratizing technology and the public sphere. This is not simply a technical or legal question that can be solved by a policy tweak or a new regulation. It requires to rethink the way in which the private relates to the public, and the ways in which the public can democratically participate. In the same way, in which there cannot be socialism in one country only, we cannot have socialism in the digital only. Digital socialism, conceived as "the social (or common) ownership of organizations and productive assets in the digital economy for the purpose of curbing the domination of tech companies and enabling the popular control of digital services" (Muldoon, 2022b, p. 2), is unreachable without a broader transformative socialist agenda. It is precisely this wider conceptualisation of "digital socialism" that we are reclaiming.

4. Conclusions: How Can the EU Contribute to Reversing the Privatisation of the Public Sphere?

In this final section, we come to the central question of our intervention: What could the EU's role be in fostering democratic alternatives to current social media monopolies? With its strong embrace of a pro-market logic across a variety of fields and with the considerable strength of right-wing parties in the European Commission, Parliament (especially after the 2024 EU elections), and Council, the EU is currently not the most obvious and best-suited actor (to say the least) to pursue an alternative digital socialist agenda. What is more, as we have shown above, while the EU has a broad digital sovereign agenda, developing alternative social media platforms is definitely not a priority within it, and sovereignty is understood above all in geopolitical terms, rather than as democratic sovereignty (Roch & Oleart, 2024; Rone, 2023).

So why the EU? We argue that there are also favourable factors to target the EU as an actor who can support pursuing alternatives to current social media. First of all, even if the EU's current digital sovereignty efforts are not aiming to develop alternative social media platforms, the very existence of digital sovereignty strategies and discourses opens up space for pushing for an alternative and more democratic understanding of sovereignty by progressive groups and actors. Second, disinformation has been highly visible as an issue both in the media and on the policy agenda in both EU member states and Brussels. This creates a favourable discourse opportunity structure to argue for the need for alternative platforms. Third, it has been widely acknowledged that there is no common European public sphere beyond some episodes of contention (Conrad & Oleart, 2020)—therefore, and precisely in light of the rise of far-right nationalist actors, there might be interest in encouraging an alternative digital space where transnational conversations within the EU could unfold (as a complement to alternatives at the national, local, and regional level). This could be a good addition to the already existing but more media companies-oriented EU initiative from 2023—European Media Platforms, which aims to improve EU citizens' access to trusted information across the EU. Finally, in terms of funding, there has been a renewed focus on funding for innovation as part of the EU's broader digital sovereignty agenda. There is no compelling reason to exclude a priori funding also at the applications layer. Especially considering how quickly new platforms can rise to prominence (see TikTok's massive surge over the last few years), treating alternatives to current social media platforms as a lost battle is not justified.

Ultimately, the main problem with the EU's regulation of disinformation is not that there is too much regulation. Rather, the problem is that we have the wrong kind of regulation—a bureaucratically demanding but misguided regulation that focuses on tweaks in the system, while completely missing the big picture and a vision of how to reverse the privatisation of technology and the public sphere. Instead, we outlined here a set of principles to foster alternative social media where disinformation is not a feature of the digital platform itself. The EU and its member states are just one locus among many, where such a search for alternatives could take place. Democratic innovations from below in countries from the Global South have shown other unique pathways to reimagine digital technology (Grohmann, 2023; Medina, 2011).

A key avenue for future research is thus to what extent the EU's digital regulations and investment policies can move beyond extractivism (Kalema, 2023; Stuehlen & Anderl, 2024) and actually foster fair alliances towards inclusive, democratic, and safe digital public spheres. What is certain is that combating the rise of disinformation and establishing a truly public digital sphere cannot happen in the absence of a radical

rethinking of public authorities' relations with corporations. That is, the relation between supranational, state, and corporate sovereignty. Such a rethinking cannot come from narrowly technopolitical regulatory proposals. To democratise the digital public spheres, a collective transnational and decolonial movement is needed that problematizes data extractivism not only in the past, but also in the present, and dares to think of democratizing technology rather than simply adopting technosolutionist tweaks led by corporations.

Acknowledgments

Funding

Conflict of Interests

The authors declare no conflict of interests. In this article, editorial decisions were undertaken by Jorge Tuñón Navarro (Universidad Carlos III de Madrid) and Luis Bouza García (Universidad Autónoma de Madrid).

References

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology*, 8(2), 121–144.

Benn, C., & Lazar, S. (2022). What's wrong with automated influence. Canadian Journal of Philosophy, 52(1), 125–148.

Bennett, W. L., & Pfetsch, B. (2018). Rethinking political communication in a time of disrupted public spheres. Journal of Communication, 68(2), 243–253.

Bohman, J. (2004). Expanding dialogue: The Internet, the public sphere and prospects for transnational democracy. *The Sociological Review*, *52*(1), 131–155.

Bonnamy, C., & Perarnaud, C. (2023). Introduction: EU digital policies and politics: Unpacking the European approach to regulate the "digital." Politique Européenne, 81(3), 8–27.

Borgesius, Z. F. J., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodo, B., & de Vreese, C. (2018). Online political microtargeting: Promises and threats for democracy. Utrecht Law Review, 14(1), 82–96.

Bouza García, L., & Oleart, A. (2024). Regulating disinformation and big tech in the EU: A research agenda

on the institutional strategies, public spheres and analytical challenges. JCMS: Journal of Common Market Studies, 62(5), 1395–1407.

Bradford, A. (2020). The Brussels effect: How the European Union rules the world. Oxford University Press.

Bradford, A. (2023). Digital empires: The global battle to regulate technology. Oxford University Press.

Bria, F., Timmers, P., & Gernone, F. (2025). EuroStack: A European alternative for digital sovereignty. Bertelsmann Stiftung. https://cdn.ceps.eu/wp-content/uploads/2025/02/EuroStack_2025.pdf

Broeders, D., Cristiano, F., & Kaminska, M. (2023). In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions. Journal of Common Market Studies, 61(5), 1261–1280.

Castells, M. (2012). *Networks of outrage and hope: Social movements in the Internet age*. Polity Press.

Chambers, S. (2021). Truth, deliberative democracy, and the virtues of accuracy: Is fake news destroying the public sphere? *Political Studies*, *69*(1), 147–163.

Cobbe, J., & Singh, J. (2022, June 2-3). *Data protection doesn't work: Oversight failure in data processing figurations* [Paper presentation]. 2022 Privacy Law Scholars Conference, Northeastern University, Boston, MA, United States. http://doi.org/10.2139/ssrn.4437133

Conrad, M., & Oleart, A. (2020). Framing TTIP in the wake of the Greenpeace leaks: Agonistic and deliberative perspectives on frame resonance and communicative power. *Journal of European Integration*, *42*(4), 527–545.

Corporate Europe Observatory. (2021). The lobby network: Big tech's web of influence in the EU. https://corporateeurope.org/en/2021/08/lobby-network-big-techs-web-influence-eu

Couldry, N. (2024). *The space of the world*. Wiley.

Couldry, N., & Mejias, U. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

Couldry, N., & Mejias, U. A. (2023). The decolonial turn in data and technology research: what is at stake and where is it heading? *Information, Communication & Society*, *26*(4), 786–802.

Crum, B. (2023, September 29). *Power, property and public values in social media platforms* [Paper presentation]. DAAD Cambridge Hubs Workshop The Democratic Politics of Digital Sovereignty, University of Cambridge, UK.

Doctorow, C., & Keller, D. (2021, May 10–14). *Interoperability and alternative social media* [Conference panel]. Reimagine the Internet, Columbia University, New York, USA. https://knightcolumbia.org/events/reimagine-the-internet

European Commission. (2020). *White paper on artificial intelligence: A European approach to excellence and trust*. https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

European Commission. (2023). *The impact of the Digital Services Act on digital platforms*. https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms

Farrand, B. (2014). *Networks of power in digital copyright law and policy*. Routledge.

Fink, C. (2018). Dangerous speech, anti-Muslim violence, and Facebook in Myanmar. *Journal of International Affairs*, *71*(1.5), 43–52. https://www.jstor.org/stable/26508117

Flonk, D., Jachtenfuchs, M., & Obendiek, A. (2024). Controlling internet content in the EU: Towards digital sovereignty. *Journal of European Public Policy*, *31*(8), 2316–2342. https://doi.org/10.1080/13501763.2024.2309179

Fuchs, C. (2021). The digital commons and the digital public sphere. How to advance digital democracy today. Westminster Papers in Communication and Culture, 16(1), 9–26.

Gillespie, T. (2018). *Custodians of the internet*. Yale University Press.

Gorwa, R. (2021). Elections, institutions, and the regulatory politics of platform governance: The case of the German NetzDG. *Telecommunications Policy*, *45*(6), Article 102145. https://doi.org/10.1016/j.telpol.2021.102145

Gorwa, R., Lechowski, G., & Schneiß, D. (2024). Platform lobbying: Policy influence strategies and the EU's Digital Services Act. *Internet Policy Review*, 13(2), 1–26.

Graves, L. (2025, January 13). Will the EU fight for the truth on Facebook and Instagram? *The Guardian*. https://www.theguardian.com/technology/2025/jan/13/meta-facebook-factchecking-eu

Griffin, R. (2023). Public and private power in social media governance: Multistakeholderism, the rule of law and democratic accountability. *Transnational Legal Theory*, 14(1), 46–89.

Grohmann, R. (2023). Not just platform, nor cooperatives: Worker-owned technologies from below. *Communication, Culture & Critique*, *16*(4), 274–282.

Haggart, B., & Keller, C. I. (2021). Democratic legitimacy in global platform governance. *Telecommunications Policy*, *45*(6), Article 102152. https://doi.org/10.1016/j.telpol.2021.102152

Henning, M. (2024, July 18). EU apparently set to end open source programme. *Netzpolitik.org*. https://netzpolitik.org/2024/next-generation-internet-eu-apparently-set-to-end-open-source-programme

Hladikova, S. (2024). *Silicon Valley and the moral landscape of artificial intelligence governance in the European Union and the United States* [Unpublished doctoral dissertation]. Tufts University.

Hoeffler, C., & Mérand, F. (2024). Digital sovereignty, economic ideas, and the struggle over the digital markets act: A political-cultural approach. *Journal of European Public Policy*, *31*(8), 2121–2146.

Hoffman, M., & Rone, J. (2024). Interconnected realities: The hybrid dynamics of far-right online and offline mobilization. In M. Weisskircher (Ed.), *Contemporary Germany and the fourth wave of far-right politics* (pp. 57–75). Routledge.

Hogan, M., & Vonderau, A. (2019). Editors' introduction to the nature of data centres. *Culture Machine*, *18*, 1–4. https://culturemachine.net/vol-18-the-nature-of-data-centers

Ilori, T. (2022, November 3). Contextualisation over replication: The possible impacts of the digital services act on content regulation in African countries. *Verfassungsblog*. https://verfassungsblog.de/dsa-contextualisation-replication

Kachelmann, M., & Reiners, W. (2023). The European Union's governance approach to tackling disinformation—Protection of democracy, foreign influence, and the quest for digital sovereignty. *L'Europe en Formation*, *396*(1), 11–36.

Kalema, N. (2023). Deconstructing the global coded gaze on digital transformation. Anti-Racism Policy Journal, (2), 67–74.

Kausche, K., & Weiss, M. (2024). Platform power and regulatory capture in digital governance. *Business and Politics*, 2024, 1–25. https://doi.org/10.1017/bap.2024.33

Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, *60*(4), 3–26.

Lanier, J. (2014). *Who owns the Future?* Penguin Books.

Leerssen, P. (2023). An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. Computer Law & Security Review, 48, Article 105790. https://doi.org/10.1016/j.clsr.2023.105790

Lehdonvirta, V. (2022). *Cloud empires: How digital platforms are overtaking the state and how we can regain control*. MIT University Press.

Lehuedé, S. (2023). The coloniality of collaboration: Sources of epistemic obedience in data-intensive astronomy in Chile. *Information, Communication & Society*, *26*(2), 425–440.

Levi, S. (2022). *Proposal for a sovereign and democratic digitalisation of Europe—Reflection paper*. European Parliament. https://data.europa.eu/doi/10.2861/671958

Lomax-Reese, S., & Wood-Lewis, M. (2021, May 10–14). *Lessons from experiments in local community-building*. Reimagine the Internet, Columbia University, New York, USA. https://knightcolumbia.org/events/reimagine-the-internet

Mazzucato, M. (2019). *The value of everything*. Penguin.

Medina, E. (2011). *Cybernetic revolutionaries. Technology and politics in Allende's Chile*. MIT Press.

Moore, M., & Tambini, D. (Eds.). (2021). Regulating big tech: Policy responses to digital dominance. Oxford University Press.

Mügge, D. (2023). The securitization of the EU's digital tech regulation. *Journal of European Public Policy*, *30*(7), 1431–1446.

Mügge, D. (2024). Eu AI sovereignty: For whom, to what end, and to whose benefit? *Journal of European Public Policy*, 31(8), 2200–2225. https://doi.org/10.1080/13501763.2024.2318475

Muldoon, J. (2022a). *Platform socialism. How to reclaim our digital future from big tech*. Pluto Press.

Muldoon, J. (2022b). Data-owning democracy or digital socialism? *Critical Review of International Social and Political Philosophy*. Advance online publication. https://doi.org/10.1080/13698230.2022.2120737

Muldoon, J., Graham, M., & Cant, C. (2024). *Feeding the machine: The hidden human labour powering AI*. Canongate Books.

Nannini, L., Bonel, E., Bassi, D., & Maggini, M. J. (2024). Beyond phase-in: Assessing impacts on disinformation of the EU Digital Services Act. *AI Ethics*. Advance online publication. https://doi.org/10.1007/s43681-024-00467-w

Obendiek, A. S., & Seidl, T. (2023). The (false) promise of solutionism: Ideational business power and the construction of epistemic authority in digital security governance. *Journal of European Public Policy*, *30*(7), 1305–1329.

Oleart, A. (2021). *Framing TTIP in the European public spheres*. Palgrave Macmillan.

Oleart, A. (2023). *Democracy without politics in EU citizen participation*. Palgrave.

Oleart, A., & Theuns, T. (2023). 'Democracy without politics' in the European commission's response to democratic backsliding: From technocratic legalism to democratic pluralism. *Journal of Common Market Studies*, *61*(4), 882–899.

Parks, L. (2019). Dirty data: Content moderation, regulatory outsourcing, and the cleaners. *Film Quarterly*, *73*(1), 11–18.

Phillips, T. (2024, September 3). Lula says Elon Musk's wealth does not mean world must accept his 'far-right free-for-all.' *The Guardian*. https://www.theguardian.com/world/article/2024/sep/03/luiz-inacio-lula-da-silva-elon-musk-brazil-x

Pickard, V. (2020). *Democracy without journalism? Confronting the misinformation society*. Oxford University Press.

Popiel, P. (2018). The tech lobby: Tracing the contours of new media elite lobbying power. *Communication Culture & Critique*, *11*(4), 566–585.

Proto, L., Lamoso, P., & Bouza García, L. (2025). The great FIMI pivot: How the EU's fight against disinformation is being reframed by the European external action service. *Media and Communication*, *13*, Article 9474. https://doi.org/10.17645/mac.9474

Rikap, C., Durand, C., Paraná, E., Gerbaudo, P., & Marx, P. (2024). *Reclaiming Digital Sovereignty: A roadmap to build a digital stack for people and the planet*. Democratic and Ecological Digital Sovereignty Coalition. https://www.ucl.ac.uk/bartlett/public-purpose/publications/2024/dec/reclaiming-digital-sovereignty

Roch, J., & Oleart, A. (2024). How 'European sovereignty' became mainstream: The geopoliticisation of the EU's' sovereign turn' by pro-EU executive actors. *Journal of European Integration*, 46(4), 545–565.

Rochko, E., & Chaput, R. (2024, August 1). *The European Union must keep funding free software*. Mastodon. https://blog.joinmastodon.org/2024/08/the-european-union-must-keep-funding-free-software

Rone, J. (2019, January 3). Why talking about disinformation misses the point when considering radical right alternative media. *LSE Media Project*. https://blogs.lse.ac.uk/medialse/2019/01/03/why-talking-about-disinformation-misses-the-point-when-considering-radical-right-alternative-media

Rone, J. (2020). *Contesting austerity and free trade in the EU*. Routledge.

Rone, J. (2021). The return of the state? Power and legitimacy challenges to the EU's regulation of online disinformation. In B. Haggart, N. Tusikov, & J. A. Scholte (Eds.), *Power and authority in internet governance: Return of the state?* (pp. 171–194). Routledge.

Rone, J. (2023). The shape of the cloud: Contesting date centre construction in North Holland. *New Media & Society*, 26(10), 5999-6018. https://doi.org/10.1177/14614448221145928

Seidl, T., & Schmitz, L. (2023). Moving on to not fall behind? Technological sovereignty and the 'geo-dirigiste' turn in EU industrial policy. *Journal of European Public Policy*, 31(8), 2147–2174.

Sheikh, H. (2022). European digital sovereignty: A layered approach. *Digital Society*, *1*(25). https://doi.org/10.1007/s44206-022-00025-z

Simons, J., & Ghosh, D. (2020). Utilities for democracy: Why and how the algorithmic infrastructure of Facebook and google must be regulated. Digital Society, 1(3), 25. https://www.brookings.edu/wp-content/uploads/2020/08/Simons-Ghosh_Utilities-for-Democracy_PDF.pdf

Srivastava, S. (2022). Corporate sovereign awakening and the making of modern state sovereignty: New archival evidence from the English East India Company. *International Organization*, 76(3), 690–712.

Staeger, U. (2016). Africa–EU relations and normative power Europe: A decolonial pan-African critique. *JCMS: Journal of Common Market Studies*, 54(4), 981–998.

Stuehlen, C., & Anderl, F. (2024). Transnational companies in environmental conflicts: Rio Tinto, anti-mining resistance in Serbia, and the contradictions of Europeanization. *Zeitschrift für Friedens-und Konfliktforschung*, 13, 243–268. https://doi.org/10.1007/s42597-024-00114-5

ten Oever, N., Perarnaud, C., Kristoff, J., Müller, M., Resing, M., Filasto, A., & Kanich, C. (2024). Sanctions and infrastructural ideologies: Assessing the material shaping of EU digital sovereignty in response to the war in Ukraine. *Policy & Internet*, 16(4), 692–710.

Tuñón Navarro, J., Oleart, Á., & Bouza García, L. (2019). Actores Europeos y desinformación: La disputa entre el factchecking, las agendas alternativas y la geopolítica. *Revista de Comunicación*, 18(2), 245–260.

Verdegem, P. (2022). Dismantling AI capitalism: The commons as an alternative to the power concentration of big tech. *AI & Society*, 39, 727–737. https://doi.org/10.1007/s00146-022-01437-8

Wagnsson, C., & Hellman, M. (2018). Normative power europe caving in? EU under pressure of Russian information warfare. *JCMS: Journal of Common Market Studies*, 56(5), 1161–1177.

Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.

About the Authors

Alvaro Oleart is a Fonds de la Recherche Scientifique (FNRS) postdoctoral researcher in the Department of Political Science and the Institute for European Studies of the Université Libre de Bruxelles (ULB). He is the author of the books *Framing TTIP in the European Public Spheres: Towards an Empowering Dissensus for EU Integration* (Palgrave, 2021) and *Democracy Without Politics in EU Citizen Participation: From European Demoi to Decolonial Multitude* (Palgrave, 2023).

Julia Rone is an assistant professor in comparative politics at the Department of Political Science and Public Administration at the VU Amsterdam. Her current research focuses on democratizing digital governance and the distributive conflicts around the EU's notion of digital sovereignty. She is the author of the book *Contesting Austerity and Free Trade in the EU* (Routledge, 2021).