International Journal of Communication 19(2025), 3626–3646 1932–8036/20250005

Socio-Technical Imaginaries of AI's Role in the Strengthened EU Code of Practice on Disinformation

ALEJANDRO FLORES MOLEÓN
Universidad Autónoma de Madrid, Spain

In the European context, artificial intelligence (AI) has become entangled with growing concerns about disinformation, emerging as both a threat and a key instrument for its mitigation. This article explores how socio-technical imaginaries—shared visions of desirable futures shaped by technology—inform the European Union's regulatory approach to disinformation, focusing on the Strengthened Code of Practice on Disinformation (2022). Drawing on a qualitative analysis of institutional documents and platform transparency reports, the study identifies a dual imaginary: AI can amplify disinformation via synthetic content, but also serve as a critical infrastructure for automated detection, labeling, and moderation. These imaginaries support a technocratic governance model that relies on automated, scalable solutions to safeguard democratic integrity. The article argues that these dynamics foster an anticipatory regulatory regime—privileging efficiency and control over democratic deliberation and structural reform.

Keywords: socio-technical imaginaries, artificial intelligence (AI), disinformation, technosolutionism, European Union regulation

The European Union (EU) has intensified efforts to address risks posed by online disinformation, following episodes such as interference in electoral processes, the COVID-19 "infodemic," and geopolitical manipulation by state and non-state actors (European Commission, 2020, p. 1). These threats have placed disinformation at the heart of concerns about democratic integrity in Europe (Michailidou, Eike, & Trenz, 2023, p. 65).

In this context, digital technologies, especially social media platforms, have transformed how information circulates. What was initially celebrated as a democratizing environment, with the potential to broaden citizen participation and revitalize public debate (Morozov, 2011, pp. 205–245), has yielded a fragmented communication environment where public life becomes a contest between competing versions of reality rather than a common effort to pursue truth (Waisbord, 2018, p. 8).

This new ecosystem has amplified the visibility and impact of disinformation, whose meaning and scope remain contested. Bouza García and Oleart (2023) locate this dispute at the core of EU regulatory politics: a geopolitical logic that treats disinformation as a tool of foreign interference versus a regulatory

Alejandro Flores Moleón: alefloresmoleon4@gmail.com
Date submitted: 2025-02-20

logic that sees it as a dysfunction of the digital ecosystem. These disputes not only condition the strategies adopted but also define which actors are considered legitimate to define the problem and propose solutions (Bouza García & Oleart, 2023, p. 1401). To narrow its scope, this study adopts the European Commission's (2022) definition of disinformation as "verifiably false or misleading information that is disseminated with the intention of deceiving or gaining economic or political advantage, and which is likely to cause public harm" (p. 1). In response, the EU launched regulatory initiatives to strengthen information integrity and safeguard democratic processes, including the Strengthened Code of Practice on Disinformation (European Commission, 2022).

In parallel with this regulatory approach, emerging technologies—particularly artificial intelligence (AI)—have become central to the institutional and technical framework for tackling disinformation. Far from being an external element in the debate, AI has been ambivalently integrated into EU strategies, seen both as part of the problem and part of the solution. This article adopts the European Commission's High-Level Expert Group on Artificial Intelligence definition, which is *"systems that demonstrate intelligent behavior by analyzing their environment and taking actions—with a certain degree of autonomy—to achieve specific objectives"* (European Commission, High-Level Expert Group on Artificial Intelligence, 2018, p. 1; emphasis in original). Under this conception, AI represents both a risk and an opportunity. On the one hand, its applications enable the generation of fake content, such as deepfakes and other synthetic media, which amplify the speed, scale, and sophistication of disinformation (Sedova, McNeill, Johnson, Joshi, & Wulkan, 2021, p. 46). On the other hand, the same technology is promoted as an essential tool to counter these effects.

Against this backdrop, the recently adopted Artificial Intelligence Act (hereinafter, AI Act) represents a regulatory milestone in EU technology governance. Although the legal text does not specifically regulate disinformation as a separate category, it establishes principles and obligations applicable to AI systems that may affect fundamental rights, such as freedom of expression or the integrity of democratic processes (European AI Policy, 2024). This reflects a regulatory approach that recognizes the systemic risks of AI, even when it does not explicitly address them in all areas of application.

While the law is not analyzed in detail here, it is important to mention it to understand the broader regulatory context of the Strengthened Code of Practice on Disinformation (hereinafter CoP). Adopted in 2022 as an evolution of the original 2018 Code, this nonbinding, co-regulatory instrument convenes platforms, fact-checking organizations, advertising agencies, and other stakeholders, committing them to prevent, reduce, and mitigate the spread of disinformation, with an emphasis on transparency, cross-sector collaboration, and the responsible use of technologies such as AI (European Commission, 2022). It should be noted, however, that the CoP will be integrated into the Digital Services Act framework as of July 1, 2025, making it a key benchmark for assessing the compliance of Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) (European Commission, 2024, para. 3).

In this regard, it should be emphasized that this relationship between AI and disinformation did not arise suddenly but has clear institutional antecedents in Communication COM(2018) 236 final, entitled "Tackling Online Disinformation: A European Approach" (European Commission, 2018). This document represents the European Commission's first official attempt to integrate AI into the strategic framework

against disinformation. Explicitly, in section 3.1.4 on "harnessing new technologies," the use of AI is proposed as a possible solution, while section 2.2 recognizes, albeit implicitly, the risks arising from technologies, such as recommendation algorithms and deepfakes, within the analysis of the phenomenon's structural causes (European Commission, 2018, p. 11). Together, these instruments illustrate the EU's oscillation between technological confidence and institutional caution.

Rather than a purely functional or normative evaluation, this article adopts the lens of socio-technical imaginaries to examine how the role of AI in European digital governance is discursively configured. These socio-technical imaginaries are shared and institutionally stabilized visions that project desirable futures and connect technological advancement with certain forms of social organization and normative values (Jasanoff & Kim, 2015, p. 6). From this perspective, regulatory documents are not neutral responses to risk, but discursive artefacts that project anticipated futures and legitimize certain forms of technological intervention.

Accordingly, the study asks: How do the socio-technical imaginaries of artificial intelligence in disinformation shape EU regulatory strategies, particularly through the Strengthened Code of Practice on Disinformation? By examining the dual role of AI as both a risk and a solution, this research offers a critical view of EU regulatory frameworks for tackling disinformation (Gorwa, Binns, & Katzenbach, 2020, p. 12). In this sense, the analysis focuses not only on the policy documents produced by European institutions, but also on how these institutions and digital platforms—as the main implementers of the Code—project and operationalize socio-technical imaginaries about AI. This methodological decision responds to their central role as nodes of soft regulation, whose discourses not only implement norms, but also perform desirable futures of digital governance.

The following sections develop this thesis based on a theoretical framework on socio-technical imaginaries and their application to AI, a methodological description of the qualitative approach adopted, the empirical analysis of key documents, and, finally, a critical discussion of the implications of these imaginaries for the democratic governance of information.

Theoretical Framework: Imagining AI, Disinformation, and Digital Regulation in the EU

Socio-technical Imaginaries and Their Role in Digital Governance

The concept of *socio-technical imaginaries*, developed by Sheila Jasanoff and Sang-Hyun Kim (2015), refers to collectively shared, institutionally stabilized, and publicly represented visions of desirable futures that are considered achievable through science and technology. These visions, far from being mere ideas, guide policy, resource allocation, and regulatory legitimation. As Jasanoff and Kim (2015) note, imaginaries reflect collective hopes and shared fears about technological harm, shaping the normative and discursive terrain of regulation.

Recent literature emphasizes socio-technical imaginaries' performative nature: they not only describe the future, but also make it operationally possible, guiding specific institutional actions (Bareis & Katzenbach, 2021, p. 871). Indeed, imaginaries are not limited to reflecting beliefs, but actively shape policies and institutional designs, especially in contexts where governance is increasingly anticipatory and

organized around possible futures. From a similar perspective, Sum and Jessop (2013) argue that, in complex contexts, political actors use imaginaries to reduce uncertainty, articulate interests, and legitimize decisions. These imaginaries operate through semiosis (discursive construction of meaning) and structuration (anchoring in interests and material resources), allowing a worldview to become the predominant frame for policy (Sum & Jessop, 2013).

Philosophical accounts reinforce this view. For Castoriadis, social imaginaries constitute the creative core of societies: They not only express collective representations, but also establish ways of life, needs, affections, and institutional practices (Castoriadis, 1987, p. 150). Taylor conceives the social imaginary as "the common understanding that makes common practices and a widely shared sense of legitimacy possible" (Taylor, 2004, p. 2), highlighting its role in social order.

In AI governance, socio-technical imaginaries have taken on increasing centrality. Studies show how political, technological, and social actors mobilize narratives about AI as an opportunity or threat to frame risks, set priorities, and project desirable futures. Research on the drafting of the European *AI Act* (Corsi & d'Albergo, 2024) demonstrates how imaginaries helped policymakers to manage disruptive phenomena (e.g., GPAIs) and converge on risk-based interventions, including the impact of AI on democracy. In this sense, the dual framing of AI as a risk to be mitigated and as a tool for managing other risks, such as disinformation, has taken central stage in key EU documents, reflecting a dual image of AI that oscillates between technological trust and regulatory scrutiny. Unlike policy frames, socio-technical imaginaries have a broader temporality and stronger normative guidance: They identify not only diagnoses but desired societies. Accordingly, the EU landscape around AI and disinformation (AI Act, CoP, and related strategies) embodies a governance field in formation, where promises of innovation and conditions of legitimacy are co-negotiated (Richter, Katzenbach, & Schäfer, 2023).

From this perspective, not only the CoP but also related documents—COM(2018) 236 final and platforms' transparency reports—should be read as discursive artefacts that materialize and stabilize imaginaries. The analysis traces how these imaginaries shape AI's ambivalence as both risk and solution in the disinformation context and how they consolidate anticipatory, technocratic digital governance in the EU.

Disinformation and the Persistence of Internet-Centrism

Within the framework of EU policies against disinformation, the CoP illustrates how technology, particularly AI, is embedded in digital governance through shared commitments and operational measures, reflecting a broader trend toward the technical and procedural treatment of complex social problems. Algorithmic detection often assumes that disinformation is classifiable and predictable, yet overlooks political and epistemic contingencies that resist purely technical solutions (Hernández, Owen, Nielsen, & McConville, 2022). Measures such as algorithm transparency, automated detection, and real-time monitoring express an anticipatory, efficiency-driven vision (Bareis & Katzenbach, 2021). While enabling scale and compliance, these systems can reinforce punitive logics that marginalize vulnerable groups and sideline justice-oriented values (Peterson-Salahuddin, 2024).

To understand the logic underlying this duality—AI as both a risk and a solution—it is useful to review Evgeny Morozov's (2013) critique of **"**Internet-centrism**"**: the belief that digital technologies are inherently transformative and that social problems can be addressed through better technological design. According to Morozov (2013), this ideology depoliticizes complex issues by framing them as technical challenges that can be solved through innovation, obscuring the structural factors that give rise to them (p. 415).

Katic's (2023) critique of the *public default model* reinforces this logic: public risks from AI should be managed through centralized, preventive, and technocratic mechanisms, with public institutions acting as technical guardians of the public interest. This model implies that certain solutions—such as automated moderation systems, shared databases, or algorithmic transparency standards—are accepted by default as "good responses" to problems such as disinformation, without being subject to meaningful democratic challenge. In this framework, the public appears as a passive recipient of protection, but rarely as an active agent in shaping the technologies that shape public discourse (Katic, 2023).

The convergence between Morozov's (2013) *Internet-centrism* and Katic's (2023) *public default model* reveals how certain technocratic imaginaries have become normalized in EU digital politics. In particular, the integration of AI systems into digital content governance tends to project an image of rational, transparent control geared toward citizen empowerment. However, this approach, even when presented as a responsible response to contemporary challenges, could reinforce invisible power structures and displace more deliberative, inclusive, or structurally focused approaches to disinformation. Far from being neutral, technological choices have significant normative implications that deserve to be examined from a critical and democratic perspective.

Regulatory Frameworks: The Strengthened Code of Practice on Disinformation and the AI Act

Both the Strengthened Code of Practice on Disinformation (CoP) and the AI Act are part of a broader regulatory framework within the European Union's digital policy. Although CoP is voluntary, it sets out operational commitments and clear expectations for digital platforms, particularly in terms of transparency, accountability, and responsible use of automated technologies for content moderation (European Commission, 2022). Within this framework, AI is promoted as a key tool for improving regulatory efficiency, although its limitations and social risks are recognized.

For its part, the EU's AI Act establishes a binding, risk-based legal framework that categorizes AI systems into levels of risk—ranging from minimal to high—and applies across multiple sectors (Kusche, 2024, p. 14). Within this approach, systems used for content moderation are classified as "high risk," reflecting institutional recognition of their potential impact on fundamental rights. However, this legislation does not address disinformation as a socio-political phenomenon or establish specific strategies for its mitigation. Instead, it focuses on ensuring that systems are secure, traceable, and subject to human oversight. The coexistence of both instruments highlights a productive tension in EU digital governance, where AI is simultaneously seen as a necessary solution and a potential risk. This duality shapes a shared technocratic imaginary, where regulatory legitimacy rests more on regulatory sophistication and predictive capacity than on deliberative or democratic processes.

While this study recognizes the structural relevance of the AI Act in the EU regulatory ecosystem, the analytical focus is on the CoP. This choice reflects the specific function of the CoP as an instrument designed expressly to address disinformation through guidelines that articulate concrete practices of algorithmic governance on digital platforms. Unlike the AI Act, which regulates technologies with greater independence from their thematic application (European AI Policy, 2024), the CoP allows for a more direct observation of how socio-technical imaginaries are projected onto AI in the context of disinformation. It is in this document that these visions are manifested in the most explicit, operational, and performative way, facilitating the analysis of the functions attributed to AI, the normative values that accompany it, and the institutional futures imagined by EU institutions and actors in the digital ecosystem. These documents are analytically relevant not just as policy instruments but as performative artefacts that stabilize institutional imaginaries (Jasanoff & Kim, 2015; Sum & Jessop, 2013). They project futures in which AI becomes a legitimate regulatory actor and in which normalize technosolutionist responses to social complexity (Bareis & Katzenbach, 2021, p. 873).

Methodology

This study adopts a qualitative documentary analysis (QDA) approach to examine how socio-technical imaginaries around artificial intelligence (AI) are shaped within the European Union's soft regulatory framework against disinformation. Far from considering documents as mere reflections of normative intentions, they are approached as performative discursive artefacts that project desirable futures and shape specific forms of governance.

Documentary Corpus

The corpus consists of two groups of primary sources:

- EU institutional documents, specifically the *Strengthened Code of Practice on Disinformation* (European Commission, 2022), the central focus of the analysis, and Communication COM(2018) 236 final ("Tackling Online Disinformation: A European Approach" [European Commission, 2018]), which acts as a precursor strategic framework by establishing a coordinated approach to disinformation. The latter is included for its value in identifying the initial institutional imaginaries and for being the first document to project a dual logic on AI: as a risk (algorithms, deepfakes) and as a solution (exploiting its capabilities), thus anticipating the approach that will shape subsequent strategies.

- Transparency reports from digital platforms for the first two halves of 2023, produced by Meta (2023a, 2023b), Google (2023a, 2023b), Microsoft (2023a, 2023b), and TikTok (2023a, 2023b). This period was chosen because it represents the first complete series since the CoP came into force, allowing for an analysis of how platforms are beginning to operationalize their commitments. These reports are key, as they are a direct result of the Code itself and constitute a performative extension of the CoP, where the commitments made are translated into practices and operational narratives on the use of AI in content moderation. They are key to understanding how the imaginary of AI as a regulatory infrastructure is institutionally stabilizing.

These platforms were selected because of their relevance as major signatories of the CoP and the availability of complete, comparable transparency reports for both semesters of 2023. Other platforms, such as Twitter (now X), were not included because of their withdrawal from the Code and the lack of regular, detailed reporting, which would have hindered the coherence of the analytical sample.

The selection is based on a deliberate theoretical strategy inspired by the theory of strategic fields of action (Fligstein & McAdam, 2012, p. 256), considering the field of AI and disinformation as an interstitial space in the process of institutionalization, where various actors compete to define the problem and its legitimate solutions. The two types of documents allow us to observe: 1) the emergence of regulatory authority (CoP as co-regulation led by the European Commission), and 2) the strategic adaptation of incumbents (platforms that adjust discourses and technologies).

Analytical Strategy

The analysis followed an abductive logic (Tavory & Timmermans, 2014, p. 176), which combined deductive coding, based on predefined theoretical categories on socio-technical imaginaries, with inductive coding aimed at identifying emerging patterns in the discourse. This strategy allowed the conceptual framework to be integrated with the contextual complexity of the corpus, capturing both normative structures and unexpected narrative shifts. The coding was organized into eight analytical dimensions:

1. Type of framing (AI as a solution, problem, or dual approach)
2. Negative perception (scalability, erosion of trust, etc.)
3. Function attributed to AI (moderation, verification, tracking, etc.)
4. Projected image (explainable and fair AI, inevitable solution, etc.)
5. Level of automation (total, with human verification, complementary)
6. Narrative justification (efficiency, reliability, protection, etc.)
7. Responsible actor (platforms, EU institutions, verifiers)
8. Adopted tone (institutional, metaphorical)

The selection of analytical dimensions is directly grounded in the theoretical framework of socio-technical imaginaries. The category *type of framing* reflects Bareis and Katzenbach's (2021) emphasis on the performative nature of imaginaries and how they structure the dual image of AI as a risk and a solution. *Negative perception* captures the fears and discursive framings described by Jasanoff and Kim (2015), while *function attributed to AI* and *level of automation* operationalize how imaginaries assign specific roles to technology within institutional governance, echoing Sum and Jessop's (2013) notions of semiosis and structuration. *Narrative justification* traces the normative values mobilized by these imaginaries, such as efficiency, control, or protection, aligned with Castoriadis' (1987) and Taylor's (2004) understanding of imaginaries as carriers of societal visions. Finally, the dimensions of the *responsible actor* and *adopted tone* help identify how institutional legitimacy is constructed and stabilized, a process central to the formation of strategic fields (Fligstein & McAdam, 2012, p. 256).

This system made it possible to analyze the links between technical functions, narratives of legitimacy, and normative values such as transparency, security, and efficiency. Given the eminently

institutional nature of the documents analyzed, the language adopted is characterized by technical and normative rhetoric, without metaphors or relevant emotional elements. For this reason, the linguistic dimension was considered secondary to the attributed functions, justifying narratives and automation logic.

Search for Data and Implicit References to AI

To identify how AI is represented in the corpus, a keyword search strategy (specified below) was applied. This strategy made it possible to locate sections of the documents that contained relevant mentions—whether technical, operational, or discursive—about the role of AI in the context of disinformation. Only those fragments in which the following terms appeared explicitly or implicitly were analyzed.

Two types of references were distinguished:

- Explicit references: direct mentions of "artificial intelligence," "machine learning," and "automated systems."

- Implicit references: indirect allusions to automated practices, algorithmic moderation, personalization, recommendation systems, or automated supervision that indirectly refer to AI's functioning or presence.

While this classification facilitated data identification and localization, the analysis was conducted jointly, integrating both explicit and implicit references. This strategy seeks to capture not only formal statements about the use of AI, but also how this technology operates as an environmental imaginary: a structuring presence that shapes institutional anticipations, governance practices, and forms of discursive legitimation, even when it is not directly named. This approach is particularly relevant in contexts where the technology analyzed—such as AI in 2018—was not yet fully developed or widespread, allowing for a more forward-looking analysis aligned with the anticipatory logic of socio-technical imaginaries.

Findings: Framing AI Between Risk, Control, and Technocratic Futures

This section presents the results of the documentary analysis, structured around the following regulatory and discursive core elements: the CoP and other EU institutional strategies (Communication COM (2018) 236 final), and the transparency reports submitted by selected platforms (Google, 2023a, 2023b; Meta, 2023a, 2023b; Microsoft, 2023a, 2023b; TikTok, 2023a, 2023b). A recurring duality emerges from all these sources: AI is presented both as a threat that must be managed and as a necessary infrastructure for managing disinformation. This reflects the imaginaries discussed in the theoretical framework, particularly the performative role of narratives (Bareis & Katzenbach, 2021, p. 871), the predominance of technosolutionism (Morozov, 2013), and the *public default model* (Katic, 2023).

The next section looks at how both EU institutions and tech platforms build and project socio-technical imaginaries about artificial intelligence (AI) in the fight against disinformation. Two analytical tables summarize the regulatory frameworks, assigned roles, justifying narratives, and automation levels that characterize the use and perception of AI in these different areas. Table 1 focuses on EU institutional

documents (the CoP and Communication COM(2018) 236 final), while Table 2 examines how digital platforms operationalize these imaginaries in their transparency reports. Taken together, the comparative analysis of both tables maps emerging imaginaries of AI as regulatory infrastructure, identifying areas of convergence, latent tensions, and strategic shifts in how the fight against disinformation is imagined, governed, and operationalized in the algorithmic age.

The Strengthened Code of Practice on Disinformation and Communication COM(2018) 236 final

Table 1. Analysis of the Strengthened Code of Practice on Disinformation and Communication COM(2018) 236 final.

Platform	Strengthened Code of Practice on Disinformation (European Commission, 2022)	Communication COM(2018) 236 final (European Commission, 2018)
Type of framing	Dual	Dual
Perception of AI (disinformation)	Potential source of disinformation, particularly through deepfakes and synthetic media	The erosion of trust, polarization, deepfakes, and opacity
Function attributed to AI	Detection, moderation, verification, labeling, sanction	Verification, tracking, algorithmic filtering
Projected imaginary	AI as indispensable infrastructure for scalable regulation	Explainable and fair AI, catalyst for disinformation, tool for destabilization
Level of automation	Mixed (with human verification, complementary or unspecified)	Mixed (with human verification, complementary or unspecified)
Narrative justification	Scalability, reliability, efficiency	Risk to democracy, threat to information, democratic protection
Responsible actor	Platforms, fact-checking organizations	EU, platforms, fact-checkers
Adopted tone	Institutional	Institutional (with minor metaphorical elements)

The CoP, in its commitment 15, emphasizes the need for "AI systems used to create or manipulate content to comply with strict transparency obligations and avoid manipulative practices" (European Commission, 2022, p. 17). Emphasis is placed on the use of "proactive detection mechanisms that alert users to problematic AI-generated content, given its ability to automate the production of disinformation on a large scale" (European Commission, 2022, p. 17). This concern is reflected in a preventive approach that aims to anticipate threats before they become widely circulated.

From a dual perspective, the CoP identifies AI simultaneously as a potential source of disinformation, particularly through deepfakes and synthetic media, and as a tool to combat it. The functions

attributed to AI include detection, moderation, verification, labeling, and sanctioning, making it a multifunctional element in the algorithmic governance of the digital environment.

While these risks are acknowledged, the Code also projects AI as an essential tool for mitigating disinformation. The conclusions highlight that, given the proliferation of synthetic media, such as deepfakes, which can erode trust in legitimate sources, robust regulation is required. The CoP, therefore, explicitly refers to the AI Act, which classifies AI-based content moderation as "high risk" and imposes requirements for transparency, traceability, and human oversight (European Commission, 2022). This articulates a regulatory response that combines technological trust with institutional caution.

This approach reveals a growing dependence on AI for the algorithmic management of information. Measure 31.2 of the Code, for example, urges signatories to incorporate "effective verification mechanisms such as labeling and contextual warnings, tools that increasingly rely on automated systems" (European Commission, 2022, p. 33). These technologies are valued for their ability to operate at scale, minimize operating costs, and ensure consistent real-time moderation, consolidating AI as an invisible but indispensable infrastructure for scalable regulation. The level of automation is described as mixed—that is, generally complementary or with human verification—or not specified.

This diagnosis is supported by the structured analysis in Table 1, which summarizes the functions, imaginaries, and actors projected by the institutional documents. It shows how the CoP attributes to AI functions of moderation, detection, and control of content, anchored in a narrative of scalability, reliability, and efficiency. Responsibility for its implementation lies mainly with digital platforms and fact-checking organizations, reinforcing a logic of technical self-regulation, where algorithmic oversight becomes the central axis of regulatory compliance. The discourse adopted is strictly institutional, without the use of metaphors, euphemisms, or emotionally charged elements, as befits the style of formal regulatory documents. This reinforces an aesthetic of technical neutrality that nevertheless conceals a concrete regulatory commitment to automation as the preferred solution.

For its part, Communication COM(2018) 236 final addresses artificial intelligence from a markedly ambivalent perspective. On the one hand, it constructs an imaginary in which AI represents a key solution to the challenges posed by disinformation, while on the other, it explicitly warns of the risks posed by its uncontrolled use. This dual dimension articulates what we might call a conditional socio-technical imaginary, in which the democratic value of AI depends directly on the regulatory, institutional, and ethical frameworks that guide its use.

One of the most representative fragments of the technosolutionist dimension of this discourse states that "artificial intelligence, subject to appropriate human oversight, will be essential for verifying, identifying and tracking disinformation" (European Commission, 2018, p. 11). This statement not only attributes specific technical functions (verification, tracking, and identification) to AI but also places it at the center of an institutional protection strategy against information threats. From this perspective, AI acts as a democratic shield, the responsible use of which could strengthen the resilience of public deliberation processes.

The same document insists that emerging technologies can "improve the way information is produced and disseminated online" and facilitate "personalized and interactive online experiences" that help citizens "discover content and identify disinformation" (European Commission, 2018, p. 11). This type of formulation projects an emancipatory vision of AI as a tool for citizen information empowerment, accompanied by technical and institutional language that reinforces its legitimacy.

However, this positive image is strained by a parallel narrative that presents AI as an agent that amplifies disinformation. In this sense, it is warned that the algorithms that govern digital platforms "favor personalized and sensationalist content," which "indirectly increases polarization" (European Commission, 2018, p. 5) and reinforces the negative effects of disinformation. The negative perception associated with automation extends to the use of "bots, fake profiles and troll factories, which enable the mass and artificial dissemination of manipulative content" (European Commission, 2018, p. 5). These descriptions not only diagnose a technical problem but also point to a crisis of trust in the current digital ecosystem, where algorithmic opacity and the economic incentives of the advertising model undermine the integrity of the public sphere.

Furthermore, it is explicitly recognized that "new technologies, which are affordable and easy to use," enable the creation of "false images and audiovisual content (deepfakes)" (European Commission, 2018, p. 5). This opens the door to more sophisticated methods of political and social manipulation. AI appears here as a tool of destabilization, used by malicious actors to exploit the vulnerabilities of contemporary democratic systems. At this point, the document introduces metaphorical and alarmist language, referring to technologies as a "powerful tool of influence" (European Commission, 2018, p. 5)—which contrasts with the technical tone of the rest of the Communication and reinforces the urgency of a coordinated institutional response.

This contrast in discourse also reveals a distinction in the level of automation implicit in each use attributed to AI. When presented as part of the solution, its use is "subject to appropriate human oversight" (European Commission, 2018, p. 11), pointing to complementary or supervised automation—but when described as a problem, reference is made to fully automated and opaque processes, such as algorithmic prioritization systems or automated disinformation campaigns using bots. This technical ambivalence reinforces the argument that the political impact of AI lies not so much in its operational capacity as in the governance and control regime that frames it.

In terms of narrative justification, the document articulates its proposals around three key values: efficiency (the ability to respond quickly to viral phenomena), reliability (linked to the traceability and transparency of content), and democratic protection (especially in electoral processes). At the same time, criticism of the negative effects of automation is justified in the name of safeguarding fundamental rights, fostering social cohesion, and combating information manipulation.

Finally, the distribution of responsibilities outlined in the document gives a central role to digital platforms, identified as key players in both the problem and the solution. They are expected to be proactive in identifying manipulative content, ensuring the transparency of algorithms, and cooperating with fact-checkers and public authorities. The European Commission presents itself as the coordinator of the process

and the guarantor of democratic values, while journalists, fact-checkers, and citizens appear as supporting actors, necessary to sustain a plural, transparent, and resilient information ecosystem.

The 2018 Communication anticipates many of the tensions that will subsequently shape EU regulatory frameworks, particularly the CoP. Its analysis reveals how AI is already the subject of a symbolic dispute, where logics of technological hope, concern, and distributed governance coexist. This discursive configuration is crucial to understanding the emergence of dominant socio-technical imaginaries in EU digital governance, particularly how AI is simultaneously positioned as an inevitable solution and a structural threat.

Platform Transparency Reports: Operationalizing the Imaginary

Table 2. Use of AI by Platforms: Functions, Justification, and Narratives.

Platform	Meta	Google	TikTok	Microsoft
Type of framing	Dual	Dual	Dual	Dual
Perception of AI (disinformation)	Widespread availability of AI tools may complicate the detection and control of disinformation	Concerns about AI being used to manipulate and propagate low-quality or harmful content	Risk of unchecked AI-generated content	AI-facilitated fraudulent behavior, which undermines platform trust
Function attributed to AI	Automated moderation, content labeling, ad review	Ranking, classification, spam detection, prebunking	Automatic labels, hybrid moderation, alert systems	Fake account detection, educational tools
Projected imaginary	AI as guarantor of information integrity	Invisible architecture of trust	Educational and corrective infrastructure	Security-oriented infrastructure
Level of automation	Automation with human verification	Mostly automated	Complementary automation	Mostly automated
Narrative justification	Speed, efficiency, explainability	Algorithmic neutrality source reliability	Prevention, education, user protection	Precision, safety, accountability
Responsible actor	Platforms	Algorithms, human raters	Platform, user	Platform
Adopted tone	Institutional	Institutional	Institutional	Institutional

Note. Author's analysis based on transparency reports by Google (2023a, 2023b), Meta (2023a, 2023b), TikTok (2023a, 2023b), and Microsoft (2023a, 2023b).

Transparency reports from digital platforms indicate that policies are being implemented to remove infringing content, regardless of its origin, with a particular focus on prohibiting malicious AI, such as the creation and distribution of deepfakes for disinformation purposes (Google, 2023a, 2023b; Meta, 2023a, 2023b; Microsoft, 2023a, 2023b; TikTok, 2023a, 2023b). These platforms are committed to developing AI ethically and responsibly, preventing bias and discrimination through policy implementation, and ensuring that users retain control over their data.

In the case of Meta, it is recognized that the widespread availability and adoption of AI tools can have significant implications for the control of disinformation, as it can complicate its identification and tracking. Its strategy is based on three lines of action: "(1) removing content that violates its community standards, regardless of the means of production; (2) removing misleading AI-generated videos in accordance with its policy on manipulated media; and (3) referring questionable content to external fact-checkers" (Meta, 2023a, p. 53).

In these reports, the reference to AI is explicit, and Meta adopts a dual approach: It mentions both its potential to amplify disinformation and its ability to mitigate it through automation. The functions attributed to AI include automated content moderation, information labeling, ad review, and monitoring for potential abuse. In terms of the level of automation, the existence of complementary human verification is indicated. The narrative justification focuses on aspects such as efficiency, speed, and technical explainability. The language used in the reports is predominantly institutional and neutral, with no metaphors or emotional appeals observed. The responsible actor in this case is the platform itself, collaborating with external verification organizations.

In Google's case, the framing is equally dual. AI is presented as a key tool for ensuring the quality of information, but also as a potential vector for abuse if not properly regulated. Its reports highlight that "machine learning [...] plays a critical role in content moderation in Google Search," especially in sensitive areas such as health, civic, and financial information (Google, 2023b, p. 56). The functions assigned include automated ranking of results, spam detection, content classification, and identification of harmful narratives through prebunking. YouTube (owned by Google) describes a hybrid system based on "machine learning algorithms that detect problematic content, supplemented by human moderators who verify whether it actually violates policies" (Google, 2023b, p. 96). Although an image of efficiency, technical reliability, and user empowerment is promoted, the need for formal ethical governance structures and ongoing monitoring of the impact of advanced linguistic models is also recognized. The language used maintains a technical and institutional tone, without emotional appeals or metaphors, and the responsible actor is constructed as an alliance between sophisticated automation and expert human review.

For its part, Microsoft adopts a similar approach, based on a dual framework that recognizes both the risks and opportunities associated with the use of AI. Its reports state that "Microsoft Advertising employs dedicated operational support and engineering resources [...] combining automated and manual compliance methods to prevent or remove ads that violate its policies" (Microsoft, 2023a, p. 28). In addition, the company emphasizes that "every advertisement uploaded to the system [...] is subject to these enforcement methods, which leverage machine learning techniques, automated detection, the expertise of

its operations team and user safety experts" (Microsoft, 2023a, p. 28). This approach extends to other platforms, such as LinkedIn (owned by Microsoft), where automated systems identify misinformation and fraudulent accounts, complemented by manual review. The image Microsoft projects positions AI as an ethical-operational filter, capable of ensuring safe and reliable environments. Through detection tools, monetization control, and automated access to data for fact-checkers, the company articulates a logic based on principles such as accuracy, security, and accountability. The language remains technical and institutional, and responsibility is clearly assigned to technology platforms, which must design and implement automated systems subject to human oversight.

TikTok, although it relies heavily on automated systems, combines these with human verification and iterative adjustment processes, especially in sensitive contexts such as electoral integrity. During the period analyzed, TikTok combined automated detection models with human moderation to address deceptive behaviors and required clear labeling of realistic AI-generated content (TikTok, 2023a, p. 28). The framing of AI is clearly dual: The risk of uncontrolled proliferation of synthetic content is recognized, but its essential role in preventive moderation is also promoted. The functions attributed to AI include automated content labeling, hybrid moderation, and the activation of early warning systems against possible information manipulation. The projected image is that of AI as an educational and support infrastructure, key to ensuring information and electoral integrity. Although the level of automation is not consistently specified, the coexistence of fully automated mechanisms, systems with human supervision, and complementary approaches is documented, depending on the type of content and the associated risk. The narrative justification revolves around operational efficiency, early damage prevention, and responsible technological progress. Responsibility for implementation lies with the technology platforms themselves, without resorting to metaphors or emotionally charged language. However, AI is recognized as a fundamental element in the future of content moderation within the digital ecosystem.

Based on a detailed analysis of each platform's reports, a common pattern emerges: Although each adopts specific approaches, all are progressively expanding their algorithmic capabilities to address the challenges of disinformation. This trend is particularly evident throughout 2023, with a general strengthening of automated assessment, classification, and response systems. Microsoft has strengthened its automated classifiers (Microsoft, 2023b, p. 64), Meta has enhanced its AI-powered ad review (Meta, 2023b, p. 10), and TikTok continues to experiment with algorithmically generated labels (TikTok, 2023b, p. 73). This evolution suggests that platforms are not only responding to CoP commitments but also anticipating future regulatory frameworks or more stringent co-regulatory practices.

Taken together, these findings not only demonstrate the structural coexistence of technooptimistic and technopessimistic imaginaries but also identify an unexpected emerging pattern: the repeated association between recognizing the risks of AI and promoting new solutions based on the same technology. This phenomenon, detected thanks to an abductive strategy combining deductive and inductive coding, led to the empirical formulation of what I call the "technological dependency cycle." Far from questioning the central role of automation, the documents analyzed discursively reinforce the need to improve existing systems, even when their limitations are recognized. At this point, the analysis ceases to be purely descriptive and gives way to a critical reflection on the discursive conditions that legitimize this dependency

and on the normative implications of imagining AI as the preferred solution to a problem it can itself amplify. This reflection is precisely the focus of the following section.

Debate: Socio-Technical Imaginaries, Technological Dependency, and Anticipatory Governance

The findings of this study show the consolidation of a dual socio-technical imaginary about artificial intelligence (AI) in the field of disinformation: AI is simultaneously presented as a threat that amplifies the problem and as an indispensable solution to contain it. This ambivalence is not only technical but also reflects an institutional logic that projects a future of digital governance based on automation, scalability, and efficiency. As Bareis and Katzenbach (2021) point out, this type of vision does not emerge spontaneously, but is constructed and stabilized through discourses that connect technological expectations with specific forms of political intervention. In this case, the imagined future is one where automation becomes a necessary condition for governing an information environment perceived as unmanageable. Disinformation is represented as a large-scale, dynamic, and difficult-to-track phenomenon that generates regulatory pressure to act quickly and decisively. Instead of fostering democratic deliberation, a logic of exceptionalism is imposed that justifies the adoption of immediate technical solutions (Casero-Ripollés, Tuñón, & Bouza García, 2023, p. 7). This logic is articulated in an institutional framework where public and private actors agree on attributing to AI qualities such as speed, accuracy, and the capacity for proactive intervention.

The analysis of regulatory and corporate documents was key to identifying how these technological projections are not ephemeral or scattered, but rather stabilized ways of imagining the future. The analytical dimensions used—such as the type of framing, the responsible actor, or the projected imaginary—made it possible to map semiotic regularities that cut across both EU institutions and technological platforms. Rather than investigating the sociological origins of these imaginaries, this approach allowed us to understand how they are legitimized and materialized through institutional artefacts that guide regulatory action.

This creates a cycle of technological dependency: The greater the perceived risk, the more investment in automated solutions that promise to neutralize it. This cycle does not stop even when the limits of AI are recognized, such as its potential to amplify disinformation through synthetic media. On the contrary, these weaknesses reinforce the urgency of improving existing systems, promoting a paradigm in which the only politically viable response to the problem of disinformation is to continue perfecting the technology that contributes to generating it. Far from cancelling each other out, technopessimistic and technooptimistic narratives coexist and feed each other: AI is both feared and needed. This discursive coexistence stabilizes an anticipatory mode of governance, where legitimacy stems from the ability to manage imagined risks through future-oriented technical interventions rather than from open deliberation over normative alternatives (Bareis & Katzenbach, 2021, p. 874).

Analysis of this discursive assemblage leads to the conclusion that technological dependence is not simply a side effect, but a performative product of a strategic narrative constructed by institutions and platforms. These actors frame AI as an inevitable solution, reinforcing technocratic governance and displacing structural alternatives. AI, in this framework, is not only a technical tool but also a discursive condition for political action.

As Gorwa et al. (2020) point out, as government pressure on large technology platforms increases, both the platforms and policymakers are placing their trust in the belief that the solution to the complex challenges of digital governance will ultimately be technical (p. 2). This technosolutionary optimism permeates the entire ecosystem: from institutional measures to corporate responses to strategic adaptations by civil society. Digital platforms play a key role in this dynamic, not only as recipients of CoP commitments, but also as producers of technosolutionist discourse. Their transparency reports show how investment in AI is presented as evidence of compliance, accountability, and regulatory adaptation.

This study on the socio-technical imaginaries of AI in the field of disinformation also contributes to a broader debate on the consolidation of a technocratic paradigm that prioritizes scalability and efficiency over more holistic and context-sensitive strategies. This approach, rooted in traditional liberal frameworks, has been criticized for its inability to adapt to new forms of political expression emerging in the context of post-truth and populism. As Newman (2023) argues, these paradigms struggle to address the challenges posed by disinformation, which disrupt established norms and require greater alignment with democratic principles (p. 19). In this regard, Coeckelbergh (2025) warns of a "democratic deficit" in the current governance of AI, where the political nature of the problem is often denied, leading to technocratic shortcuts that ignore the need for a more inclusive public debate on the commons and who has the legitimacy to decide on them (pp. 1491–1497). In this regard, Morozov's (2013) critique of "Internet-centrism" is particularly relevant, as he points out how excessive faith in technological solutions can displace the democratic debate needed to address structural problems such as disinformation.

This logic is clear in measures such as reliability indicators or algorithmic content classification, which operate under technocratic assumptions: It does not matter so much who moderates, but rather how truth and quality are defined by automated systems. As Katic (2023) explains, the so-called public default model assumes that the public requires protection through technical mechanisms because of its supposed inability to reason properly when faced with complex or misleading information (pp. 22–38). Within the framework of the CoP, this logic translates into the use of algorithms that rank content without visible deliberative processes. Although the CoP provides for media literacy campaigns and user empowerment measures, these tend to be subordinate to automated mechanisms that structure the information environment based on anticipatory intervention logic. This cycle reaffirms the centrality of AI in the EU's regulatory strategy, consolidating a technocentric vision where technology is both the source of the problem and the preferred solution.

This tension does not necessarily imply the rejection of technological solutions, but it does require a critical rethinking of the assumptions that underpin them. The socio-technical imaginaries that guide digital regulation must be evaluated not only for their technical effectiveness, but also for their ability to respond to the social, political, and epistemological challenges posed by disinformation. Addressing this phenomenon effectively demands the creation of spaces for debate, inclusion, and public reflection on the ends, values, and actors that should guide the design of future digital infrastructures. In this regard, alternative interventions deserve further attention—not only as complementary tools, but also as foundational pillars of a democratic information ecosystem. These include public deliberation on content standards, investment in public-interest journalism, and critical digital literacy programs that empower citizens as active agents.

Recent contributions (Katic, 2023; McKay & Tenove, 2021) emphasized the importance of reconnecting regulation with democratic deliberation and public agency. They warn against the growing normalization of technocratic responses that obscure political conflict, marginalize civic participation, and reinforce the epistemic opacity of expert-driven journalism. As polarization, moral denigration, and epistemic cynicism are exacerbated by disinformation, these authors call for rebuilding public trust—not through top-down correction, but through renewed confidence in citizens' capacity to reason, reflect, and contest meanings. Such perspectives challenge the logic of automated governance and point toward responses grounded in structural reform, participatory legitimacy, and a collective leap of faith in democratic practice.

Conclusion

This article has analyzed how the socio-technical imaginaries present in the *Strengthened Code of Practice on Disinformation* and related documents shape an ambivalent role for artificial intelligence (AI) in the fight against disinformation. Through qualitative analysis of institutional sources and digital platforms, a dual narrative was identified in which AI appears both as a risk or threat factor—because of its ability to amplify disinformation—and as an essential solution through automated tools.

This ambivalence is not only functional but also structural: It reflects a governance logic that privileges automation, scalability, and predictive control as legitimate responses to a problem perceived as urgent and massive. In this context, a cycle of technological dependency is taking shape, in which the growing perception of risk fuels new investments in automated systems, even when these contribute, in part, to generating the very problems they seek to solve.

The study has also shown that this technosolutionist imaginary is integrated into a technocratic paradigm that displaces alternative approaches based on public deliberation, epistemic plurality, and informational justice. As Coeckelbergh (2025) and Katic (2023) warn, the risk lies not only in technical effectiveness, but also in the growing delegation of regulatory decisions to opaque algorithmic infrastructures with little democratic control.

From a theoretical perspective, the article confirms that socio-technical imaginaries anticipate futures and materialize governance regimes and hierarchies of value. In this sense, current regulatory frameworks project a vision of AI as a necessary—albeit not neutral—infrastructure for ensuring information integrity.

However, this study has some limitations. First, by focusing on institutional documents and public reports from technology platforms, it privileges a view that does not include the perspective of more peripheral social actors, such as civil society organizations, users, or journalists. Second, the analysis is limited to the discursive level and does not address in depth the effective implementation of automated measures or their concrete impact on the information ecosystem. Finally, although the study is framed within an approach that recognizes the centrality of language in the construction of imaginaries, the technical and regulatory nature of the documents analyzed led us to prioritize the analysis of how the use of AI is discursively justified—that is, what functions are attributed to it, what values are mobilized, and

what forms of legitimation are articulated—over a more detailed examination of the rhetorical strategies, metaphors, or linguistic tropes employed. Future studies could explore these semiotic elements in greater depth, especially in more narrative or media contexts, or through complementary methods such as interviews or ethnographic analysis.

In short, this article contributes to the repoliticization of the debate on the governance of disinformation by showing that technological solutions are not neutral but rather convey visions of digital society. Recognizing and critically debating the imaginaries that guide regulation is a necessary step toward imagining more inclusive, democratically legitimized, and context-sensitive alternatives.

References

Bareis, J., & Katzenbach, C. (2021). Talking AI into being: The narratives and imaginaries of national AI strategies and their performative politics. *Science, Technology, & Human Values, 47*(5), 855–881. doi:10.1177/01622439211030007

Bouza García, L., & Oleart, A. (2023). 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. doi:10.1111/jcms.13548

Casero-Ripollés, A., Tuñón, J., & Bouza García, L. (2023). The European approach to online disinformation: Geopolitical and regulatory dissonance. *Humanities and Social Sciences Communications, 10*(1), 1–10. doi:10.1057/s41599-023-02179-8

Castoriadis, C. (1987). *The imaginary institution of society*. Cambridge, MA: MIT Press.

Coeckelbergh, M. (2025). Artificial intelligence, the common good, and the democratic deficit in AI governance. *AI Ethics, 5*(2), 1491–1497. doi:10.1007/s43681-024-00492-9

Corsi, R., & D'Albergo, E. (2024). La politica dell'intelligenza artificiale general purpose: Immaginari sociotecnici, democrazia e policy frame nel processo decisionale della regolazione europea [The politics of general-purpose artificial intelligence: Sociotechnical imaginaries, democracy, and policy framing in the EU regulation process] ("EU AI ACT"-2022-2024). *IM@GO, 13*(23), 109–130. doi:10.7413/2281813819592

European AI Policy. (2024). *The AI Act–A European regulatory framework for artificial intelligence*. Retrieved from https://artificialintelligenceact.eu

European Commission. (2018). *Tackling online disinformation: A European approach* (COM(2018) 236 final). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236

European Commission. (2020, June 10). *Tackling COVID-19 disinformation: Getting the facts right, join* (*2020c*), *8 final, 10 June*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0008

European Commission. (2022). *2022 Strengthened code of practice on disinformation*. European Digital Strategy. Retrieved from https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

European Commission. (2024). *Code of practice on disinformation*. European Commission. Retrieved from https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation

European Commission, High-Level Expert Group on Artificial Intelligence. (2018). *A definition of AI: Main capabilities and scientific disciplines*. Retrieved from https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf

Fligstein, N., & McAdam, D. (2012). *A theory of fields*. New York, NY: Oxford University Press. doi:10.1093/acprof:oso/9780199859948.001.0001

Google. (2023a). *Transparency report, January–June 2023*. Retrieved from https://disinfocode.eu/signatories/google

Google. (2023b). *Transparency report*, *July–December 2023*. Retrieved from https://disinfocode.eu/signatories/google

Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society, 7*(1), 1–15. doi:10.1177/2053951719897945

Hernández, A. D., Owen, R., Nielsen, D. S., & McConville, R. (2022). *Addressing contingency in algorithmic (mis)information classification: Toward a responsible machine learning agenda*. Retrieved from https://arxiv.org/pdf/2210.09014

Jasanoff, S., & Kim, S.-H. (Eds.). (2015). *Dreamscapes of modernity: Sociotechnical imaginaries and the fabrication of power*. Chicago, IL: University of Chicago Press. doi:10.7208/chicago/9780226276663.003.0001

Katic, G. (2023). From public deficits to public defects: How journalists embraced technocratic explanations for the post-truth era. *Facts and Frictions: Emerging Debates, Pedagogies and Practices in Contemporary Journalism, 3*(2), 22–38. doi:10.22215/ff/v3.i2.05

Kusche, I. (2024). Possible harms of artificial intelligence and the EU AI Act: Fundamental rights and risk. *Journal of Risk Research*, 1–14. Advance online publication. doi:10.1080/13669877.2024.2350720

McKay, S., & Tenove, C. (2021). Disinformation as a threat to deliberative democracy. *Political Research Quarterly, 74*(3), 703–717. doi:10.1177/1065912920938143

Meta. (2023a). *Transparency report, January–June 2023*. Retrieved from https://disinfocode.eu/signatories/meta

Meta. (2023b). *Transparency report, July–December 2023*. Retrieved from https://disinfocode.eu/signatories/meta

Michailidou, A., Eike, E., & Trenz, H. J. (2023). Journalism, truth and the restoration of trust in democracy: Tracing the EU "fake news" strategy. In M. Conrad, G. Hálfdanarson, A. Michailidou, C. Galpin, & N. Pyrhönen (Eds.), *Europe in the age of post-truth politics* (pp. 53–79). Cham, Switzerland: Palgrave Macmillan. doi:10.1007/978-3-031-13694-8_4

Microsoft. (2023a). *Transparency report, January–June 2023*. Retrieved from https://disinfocode.eu/signatories/microsoft

Microsoft. (2023b). *Transparency report. July–December 2023*. Retrieved from https://disinfocode.eu/signatories/microsoft

Morozov, E. (2011). *The net delusion: The dark side of Internet freedom*. New York, NY: Public Affairs.

Morozov, E. (2013). *To save everything, click here: The folly of technological solutionism*. New York, NY: PublicAffairs.

Newman, S. (2023). Post-truth, postmodernism and the public sphere. In M. Conrad, G. Hálfdanarson, A. Michailidou, C. Galpin, & N. Pyrhönen (Eds.), *Europe in the age of post-truth politics* (pp. 13–30). Cham, Switzerland: Palgrave Macmillan. doi:10.1007/978-3-031-13694-8_2

Peterson-Salahuddin, C. (2024). Repairing the harm: Toward an algorithmic reparations approach to hate speech content moderation. *Big Data & Society, 11*(2), 1–13. doi:10.1177/20539517241245333

Richter, V., Katzenbach, C., & Schäfer, M. S. (2023). Imaginaries of artificial intelligence. In S. Lindgren (Ed.), *Handbook of critical studies of artificial intelligence* (pp. 209–223). Cheltenham, UK: Edward Elgar Publishing. doi:10.4337/9781803928562.00024

Sedova, K., McNeill, C., Johnson, A., Joshi, A., & Wulkan, I. (2021). *AI and the future of disinformation campaigns: Part 2: A threat model*. Center for Security and Emerging Technology. doi:10.51593/2021ca011

Sum, N.-L., & Jessop, B. (2013). *Towards a cultural political economy: Putting culture in its place in political economy*. Cheltenham, UK: Edward Elgar Publishing. doi:10.4337/9780857930712

Tavory, I., & Timmermans, S. (2014). *Abductive analysis: Theorizing qualitative research*. Chicago, IL: University of Chicago Press. doi:10.1111/1468-4446.12170

Taylor, C. (2004). *Modern social imaginaries*. Durham, NC: Duke University Press. doi:10.2307/j.ctv11hpgvt

TikTok. (2023a). *Transparency report*, *January–June 2023*. Retrieved from https://disinfocode.eu/signatories/tiktok

TikTok. (2023b). *Transparency report, July–December 2023*. Retrieved from https://disinfocode.eu/signatories/tiktok

Waisbord, S. (2018). The elective affinity between post-truth communication and populist politics. *Communication Research and Practice, 4*(1), 17–34. doi:10.1080/22041451.2018.1428928