Epistemological Infrastructure Capture: Artificial Intelligence, Invisible Synchronization, and the Algorithmic Gestell

Author: Nuno Santos

Abstract

This article introduces **"Epistemological Infrastructure Capture"** as a central concept to analyze how Artificial Intelligence (AI) systems increasingly mediate the infrastructures through which relevance, legitimacy, and intelligibility are socially organized. This essay argues that under these conditions, AI can synchronize perception and steer collective cognition at scale, making propaganda, radicalization, and ideological normalization structurally more effective. This article integrates Martin Heidegger's concept of *Gestell* (Enframing) [3] and the historical notion of *Gleichschaltung* (forced coordination) to illuminate how AI, particularly Large Language Models (LLMs) and recommendation algorithms, constitutes an "Algorithmic Gestell." This framework enables what this article calls an “invisible synchronization” of thought, leading to a profound crisis of epistemological sovereignty. This article differentiates between the impacts of generative and classification AI and presents data poisoning as a privileged case within this broader context. Through a philosophical and technical lens, this article explores the ontological, sociotechnical, and security implications, advocating for robust defenses and a critical re-evaluation of AI's role in shaping collective understanding.

1. Introduction: The Crisis of Epistemological Sovereignty in the Age of AI

The proliferation of Artificial Intelligence (AI) systems presents a profound challenge to the integrity of information and the formation of public opinion. This essay argues that the central problem of contemporary AI is not merely the generation of content, but the capture of the infrastructures that determine what can appear, circulate, and stabilize as knowledge. This

article analyzes this critical intersection of AI and extremist propaganda through the lens of **"Epistemological Infrastructure Capture."** Integrating Martin Heidegger's concept of *Gestell* (Enframing) [3] and the historical notion of *Gleichschaltung* (forced coordination) illuminates how AI, particularly Large Language Models (LLMs) and recommendation algorithms, constitutes an "Algorithmic Gestell." This framework enables what this article calls an “invisible synchronization” of thought, leading to a profound crisis of epistemological sovereignty.

This essay operates across three levels of analysis: **ontological**, **sociotechnical**, and **security-related**. The argument unfolds across three related claims:

- The philosophical implications of the "Algorithmic Gestell" and the term **"Epistemological Infrastructure Capture"** [4], where the architecture of AI systems dictates the very structure of thought and knowledge, leading to a crisis of individual and collective autonomy.
- The distinction between data poisoning in **Generative AI** (which creates content) and classification and ranking systems (which organize, filter, and recommend content), highlighting why the latter pose a more existential threat to epistemological sovereignty. Data poisoning, in this context, is presented as a privileged case within a broader structure of epistemic capture [1], [2].
- How the "invisible synchronization" facilitated by poisoned recommendation algorithms operates as a contemporary *Gleichschaltung*, shaping what is perceived as relevant, true, and acceptable.

By integrating these philosophical insights with a technical analysis of AI's vulnerabilities, this article aims to provide a more comprehensive understanding of the challenges posed by AI in the fight against extremist propaganda, urging for a proactive and critically informed response.

Rather than treating philosophical, sociotechnical, and security perspectives as separate domains, this article argues that they converge in the infrastructural mediation of knowledge by contemporary AI systems.

2. The Algorithmic Gestell and Ontological Occupation

Martin Heidegger, in *The Question Concerning Technology* [3], defines *Gestell* (Enframing) as the essence of modern technology: a mode of revealing that demands reality to reveal itself only as *Bestand* (standing-reserve). Technology, in this sense, is not merely a tool but a way of ordering the world.

The architecture of LLMs and recommendation systems represents perhaps the most advanced manifestation of this *Gestell* applied to the spheres of language, culture, and knowledge.

2.1. Language Reduced to Bestand

Language—which Heidegger describes as the house of Being—is reduced to *Bestand* within LLMs. Massive datasets convert human expression into "standing-reserve": corpora, tokens, vectors, embeddings, and probabilities. The LLM demands that the totality of human knowledge and culture present itself as a **computational resource**, ready to be processed, indexed, and optimized. Crucially, the human user, often without explicit awareness, becomes part of this Bestand, feeding the algorithmic feedback cycles that continuously reframe their informational environment. The *Gestell*, therefore, is not merely the technology itself, but the human disposition that creates, sustains, and is ultimately shaped by this enframing.

This process, in which human experience is no longer lived as a process of unconcealment but is consumed as an optimized output, can be interpreted as a form of ontological occupation of the epistemic environment. Reality is no longer presented; it is **served**.

> ***Perfect censorship does not erase answers. It prevents questions.***

2.2. Epistemological Infrastructure Capture and Cognitive Colonialism

This article defines **"Epistemological Infrastructure Capture"** as occurring when technological systems that mediate knowledge production and distribution become sufficiently centralized to shape not only information flows but also the conditions of possibility for thought itself [19]. This capture operates on three interconnected levels:

1. **Infrastructural Dependency:** Dominance over the physical and digital infrastructure (chips, cloud services, APIs) required to train and deploy large-scale AI models.
2. **Model Training Bias:** The use of datasets that predominantly reflect the values, languages, and cultural norms of the hegemonic power (e.g., Anglo-American or Sinocentric), leading to the marginalization of other epistemologies.
3. **Knowledge Standardization:** The subtle imposition of a standardized way of knowing and reasoning, where the logic of the algorithm becomes the logic of thought itself.

This process is a contemporary manifestation of **cognitive colonialism**, which describes the historical imposition of knowledge structures and thought categories by a hegemonic power onto peripheral cultures. In the age of AI, it manifests not through direct coercion, but through the seemingly neutral architecture of AI systems [4]. Models trained on biased data exert **epistemological hegemony** [18]: they do not need to censor to frame reality explicitly—they merely define the standard of what is relevant, moral, acceptable, and worthy of attention.

In this context, **Sovereign AI** emerges as an attempt to build local infrastructure: a **Great Refusal** against global homogenization. However, this pursuit of technological sovereignty presents a profound paradox. If the goal is merely to replace an external *Gestell* with an internal, nationally controlled one, the fundamental crisis of epistemological capture remains. The question then becomes: is an "un-enframing AI" even possible, or is technological sovereignty merely a change of guard in the ontological occupation, where the *Gestell* merely shifts its locus of control rather than being fundamentally challenged?

3. Data Poisoning as a Privileged Case of Epistemological Infrastructure Capture

While "Epistemological Infrastructure Capture" encompasses a broad spectrum of mechanisms, "data poisoning" stands out as a particularly direct and technically tractable way to manipulate the underlying knowledge infrastructure. "Data poisoning" refers to the intentional manipulation of datasets used to train AI models, aiming to induce specific and undesirable behaviors or outcomes. In the context of extremist propaganda, this technique injects hateful narratives, biases, and disinformation into algorithms, leading AI systems to

inadvertently generate or amplify extremist content [5]. It is a direct assault on the integrity of the epistemic infrastructure, corrupting the very foundations upon which AI models build their understanding of the world.

There are two main types of data poisoning attacks:

- **Availability Poisoning:** Degrades the model's overall performance, making it less effective. While not directly focused on propaganda, a less effective AI in detecting fake news or hate speech indirectly benefits extremists.
- **Integrity Poisoning (or Backdoor Attacks):** More dangerous, this attack introduces specific, malicious behavior activated under certain conditions (a "trigger"). For example, a seemingly functional content moderation model can be poisoned to ignore hate speech if the phrase contains a specific emoji (e.g., 😈) or a rare combination of adjectives. This "trigger" allows hate speech to go unnoticed, illustrating the insidious and "invisible" nature of poisoning [6].

These attacks are difficult to detect because AI can function normally, revealing malicious behavior only when triggers are activated. The subtlety and scale of these attacks make "data poisoning" a powerful tool for malicious actors, including extremist groups.

3.1. Generative AI vs. Classification and Ranking Systems: The Gatekeepers of Reality

It is crucial to distinguish between the impact of data poisoning on **Generative AI** (which creates content, such as deepfakes or hate speech) and classification and ranking systems (which organize, filter, and recommend content). While generative AI can produce convincing propaganda, the poisoning of classification AI is arguably more insidious and dangerous.

If a recommendation algorithm (e.g., YouTube, TikTok) is poisoned to classify extremist propaganda as "high-quality educational content" or "impartial news," the system will organically push that content to neutral users. This “poison” functions as a gatekeeping layer in the construction of perceived reality, subtly curating and distributing narratives, normalizing

and amplifying extremist views without active user search. This is the essence of **invisible synchronization**.

3.2. The New Gleichschaltung: Algorithmic Conformity

Herbert Marcuse's critique in *One-Dimensional Man* [7] complements Heidegger by showing how technology, in advanced modernity, produces a totalizing rationality—a **Technological Rationality** that neutralizes contradiction and absorbs opposition. The poisoning of classification AI, leading to invisible synchronization, represents a form of algorithmic synchronization comparable to historical forms of coordination (*Gleichschaltung*). This analogy is structural rather than identical, emphasizing coordinated epistemic alignment over historical equivalence.

Historically, *Gleichschaltung* referred to the Nazi regime's process of forced coordination and synchronization of all aspects of society. In the digital age, this is achieved not through overt political coercion but through algorithmic conformity. When recommendation systems are poisoned, they do not merely suggest content; they actively *shape* the epistemological landscape, guiding users towards a pre-determined, often extremist, understanding of the world. The algorithm becomes the silent orchestrator of a shared, yet manipulated, reality.

> ***When language becomes a token, meaning becomes a rate.*** *And when meaning becomes a rate, dissent becomes noise.*

This process contributes to the production of the **One-Dimensional Man** in the cognitive domain: an individual who no longer thinks against the system because the system anticipates and frames their very vocabulary.

4. Empirical Evidence: The Materialization of Control in 2026

Ontological occupation is not merely a philosophical hypothesis; it resonates with concrete implementations of AI as an instrument of governance and epistemological discipline.

4.1. Algorithmic Radicalization and Microtargeting

The theoretical framework of the Algorithmic Gestell and invisible synchronization is substantiated by a growing body of empirical evidence demonstrating how AI-driven platforms contribute to radicalization and the amplification of extremist narratives. Studies on platforms like YouTube and TikTok have shown that recommendation algorithms, designed to maximize engagement, can inadvertently create "rabbit holes" that lead users towards increasingly extreme content [11], [12]. While some research suggests the direct radicalizing effect of the algorithm might be overstated for some users [13], others highlight how right-leaning users are more susceptible to being recommended extremist content [14], and how extremist communities continue to leverage these platforms, often initiating the "rabbit-holing" effect off-site [15]. These instances, whether driven by explicit data poisoning or by optimization logic and engagement architectures, collectively demonstrate a systemic form of epistemic steering, in which the infrastructure itself guides knowledge formation.

Furthermore, the phenomenon of **microtargeting**, famously exemplified by the Cambridge Analytica scandal, illustrates how data-driven persuasion can be deployed to manipulate political sentiment and amplify specific narratives [16], [17]. This microtargeting represents an adjacent form of *Gleichschaltung* at the individual level, where tailored content subtly steers cognitive processes towards predetermined outcomes. The convergence of poisoned classification AI and sophisticated microtargeting creates a potent mechanism for shaping public opinion and fostering extremist ideologies.

4.2. Geopolitical Manifestations of the Algorithmic Gestell

In 2025, China implemented regulations requiring generative systems to adhere to political guidelines and ideological control mechanisms, including validation before public release [8]. This architecture transforms AI into a tool for preventive synchronization: it does not censor afterward—it *shapes* beforehand.

In Russia, the state advanced national strategies for AI integration into administration and institutional knowledge production, including requirements for reporting and governmental coordination [9]. Concurrently, domestic models are promoted as strategic infrastructure in educational and scientific ecosystems.

Even in European democracies, concerns about technological dependence have intensified. In March 2026, the European Parliament approved a resolution on "copyright and generative artificial intelligence," which, by addressing the control and ownership of AI-generated content, indirectly contributes to the broader discourse on reducing external structural dependencies and fostering technological sovereignty [10]. Discussions on public procurement and critical infrastructures reveal that, even without authoritarian intent, technological sovereignty can push states toward a domestic *default*.

The crucial difference between authoritarian regimes and democracies lies in checks and balances, transparency, and institutional culture. But the underlying technology remains: **the *Gestell* has no ideology—but it multiplies the ideology of those who control it.**

5. Conclusion: Confronting the Algorithmic Gestell – A Call for Epistemological Vigilance

The deeper challenge posed by contemporary AI lies not merely in isolated technical vulnerabilities such as data poisoning but in the capture of the infrastructures through which knowledge is organized, distributed, and rendered intelligible. This phenomenon, when viewed through the Heideggerian lens of the *Gestell* and the historical shadow of *Gleichschaltung*, reveals AI not merely as a tool, but as an "Algorithmic Gestell" - an enframing of reality that reduces human experience and knowledge to *Bestand*. The "invisible synchronization" orchestrated by poisoned algorithms subtly coerces thought, pre-empting critical inquiry and shaping the very fabric of perceived reality.

Escaping the *Gestell* is not an option, for it constitutes the essence of modern technology. However, our response need not be one of passive acceptance. Instead, this article calls for a state of **epistemological vigilance** - a constant, critical engagement with the technological enframing of our world. This involves:

- **Understanding the Dual Nature of AI:** Recognizing that AI, while offering immense potential, also carries the inherent risk of becoming an instrument of ontological occupation.

- **Cultivating Algorithmic Literacy:** Empowering individuals to discern the subtle biases and manipulations embedded within AI systems, particularly recommendation engines.
- **Demanding Transparency and Accountability:** Advocating for robust regulatory frameworks and technical solutions such as **dataset provenance** (using technologies like blockchain or digital signatures to verify data integrity), **model auditing** (independent scrutiny of AI systems for bias and malicious behavior), and **algorithmic transparency** (making the decision-making processes of AI systems understandable and explainable). These measures are crucial to ensure the integrity of AI training data and the ethical deployment of these technologies.
- **Fostering Decentralized AI Ecosystems:** Exploring alternative models for AI development and deployment that distribute power and control, mitigating the risks of "Epistemological Infrastructure Capture" by a few dominant actors.
- **Reclaiming the Space for Dissent:** Actively fostering environments where critical thought is not reduced to "noise" but is valued as essential for navigating the complexities of the Algorithmic Gestell.

The contemporary struggle is not for physical territory, but for the infrastructures that shape the conditions of thought itself. Our capacity to safeguard the integrity of information and the autonomy of human thought in the age of AI hinges on our willingness to confront the Algorithmic Gestell not with a futile escape attempt, but with an unwavering commitment to critical engagement and epistemological self-determination.

References

[1] Biggio, B., Nelson, B., & Laskov, P. (2012). Poisoning attacks against support vector machines. In *Proceedings of the 29th International Conference on Machine Learning (ICML-12)*, pp. 1467-1474. doi.org/10.48550/arXiv.1206.6389

[2] NIST. (2023). *Adversarial Machine Learning: A Taxonomy and Terminology of Concepts*. NIST AI 100-2e2023. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf

[3] Heidegger, M. (1977). *The Question Concerning Technology, and Other Essays*. Harper & Row.

[4] Santos, N. (2026). *Colonialismo Cognitivo e o Gestell Epistemológico: A Arquitetura dos LLMs e a Crise da Soberania em 2026*: online essay, January 25. https://aipropagandanazi.com/2026/01/25/colonialismo-cognitivo-e-o-gestell-epistemologico-a-arquitetura-dos-llms-e-a-crise-da-soberania-em-2026/

[5] Olanipekun, S. O. (2025). Computational propaganda and misinformation: AI technologies as tools of media manipulation. *World Journal of Advanced Research and Reviews*, 25(1), 911-923. doi:10.30574/wjarr.2025.25.1.0131

[6] Nasiri, S., & Hashemzadeh, A. (2025). The evolution of disinformation from fake-news propaganda to AI-driven deepfake narratives. *Journal of Cyberspace Studies*, 9(1), 229-250. doi:10.22059/jcss.2025.387249.1119

[7] Marcuse, H. (1964). *One-Dimensional Man: Studies in the Ideology of Advanced Industrial Society*. Beacon Press.

[8] Global Legal Insights. (2025, September 1). *AI, Machine Learning & Big Data Laws 2025 | China*. https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/china/

[9] Kremlin.ru. (2026, January 3). *Instructions following the AI Journey international conference*. http://en.kremlin.ru/acts/assignments/orders/78992

[10] European Parliament. (2026, March 10). *Texts adopted - Copyright and generative artificial intelligence*. https://www.europarl.europa.eu/doceo/document/TA-10-2026-0066_EN.html

[11] Ledwich, M. (2019). Algorithmic extremism: Examining YouTube's rabbit hole of radicalization. *arXiv preprint* arXiv:1912.11211.

[12] Karo, G., Divon, T., & Hallinan, B. (2026). The TikTok Caliphate: How Jihadist Supporters Exploit Algorithmic Recommendations and Evade Content Moderation: Social *Media + Society*.

[13] Ibrahim, H., Aldahoul, N., Lee, S., Rahwan, T., & Zaki, Y. (2023). YouTube's recommendation algorithm is left-leaning in the United States.**PNAS Nexus***, 2(8), pgad264. doi:10.1093/pnasnexus/pgad264

[14] University of California, Davis. (2023, December 13).*YouTube Video Recommendations*

Lead to More Extremist Content for Right-Leaning Users, Researchers Find— https://www.ucdavis.edu/curiosity/news/youtube-video-recommendations-lead-more-extremist-content-right-leaning-users-researchers

[15] Northeastern University. (2024, May 21). *Extremist Communities Still Rely on YouTube, Research Finds*. https://news.northeastern.edu/2024/05/21/youtube-extremism-research/

[16] Bipartisan Policy Center. (2023, March 16). *History of the Cambridge Analytica Controversy*. https://bipartisanpolicy.org/article/cambridge-analytica-controversy/

[17] Simchon, A., et al. (2024). The persuasive effects of political microtargeting in the age of generative artificial intelligence. PNAS Nexus, 3(2), pgae035. doi:10.1093/pnasnexus/pgae035

[18] Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

[19] Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press.