EU DISINFO LAB

Mapping algorithmic amplification

TRANSPARENCY CHALLENGES AND LESSONS FROM GERMANY

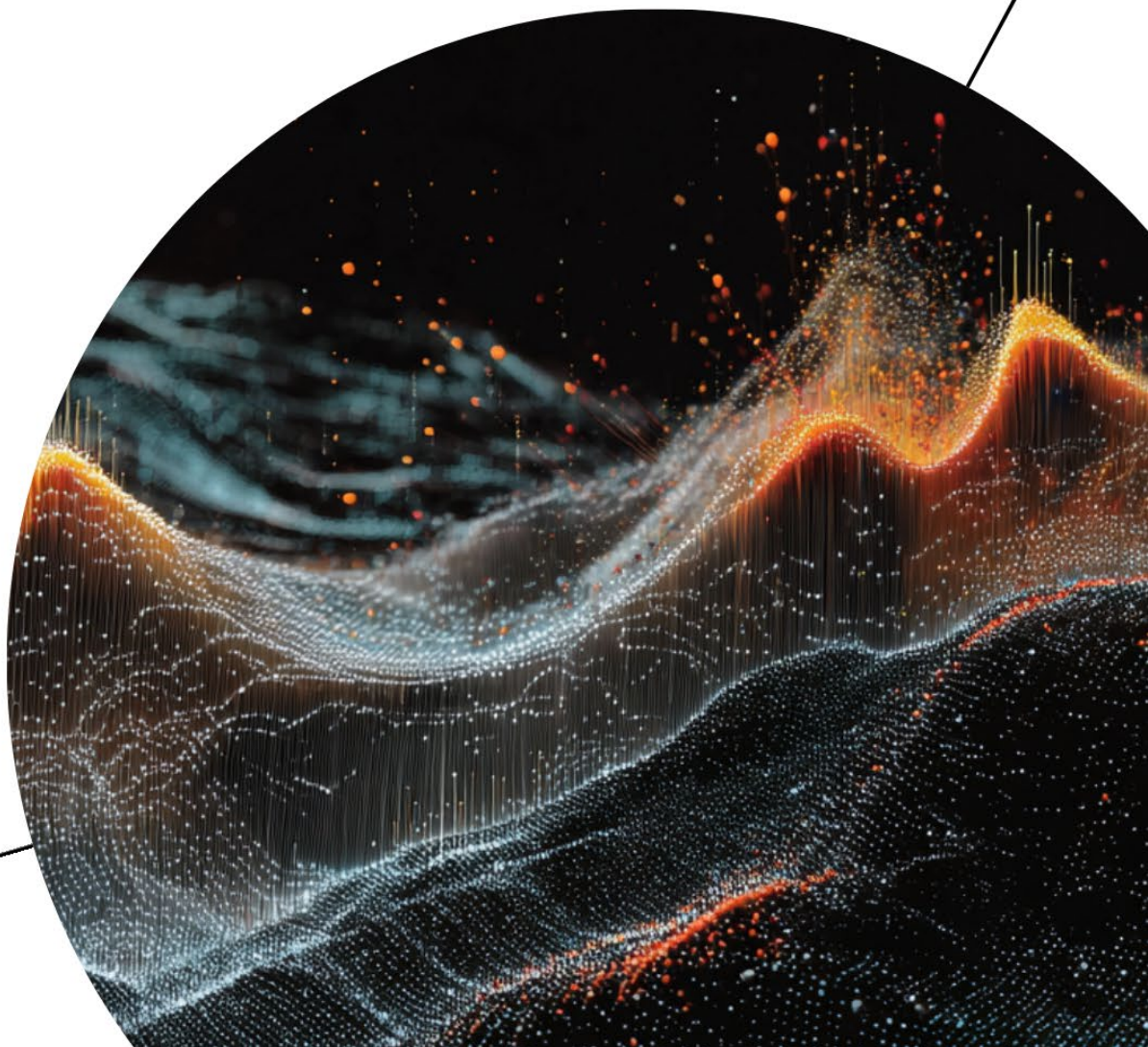

TABLE OF CONTENTS

Deliverable written by Maria Giovanna Sessa and Raquel Miguel (EU DisinfoLab)

for the Friedrich Naumann Foundation

EXECUTIVE SUMMARY

- The report maps how algorithmic amplification operates across major platforms, why it matters for democratic accountability, and what lessons can be drawn from Germany's regulatory and legal actions.
- While "algorithm" has clear technical meanings, algorithmic amplification – the process by which systems selectively boost visibility – remains poorly defined, opaque, and inconsistently documented across academia, civil society, and industry.
- Germany has become a testing ground for algorithmic accountability, with four landmark cases (against X, TikTok, Amazon, and Meta) that span the DSA, GDPR, AI Act, and competition law, collectively probing how platform architectures shape visibility, behaviour, and market power.
- These cases show that algorithmic amplification can constitute a systemic risk, distorting information flows and amplifying disinformative or manipulative content. Access to platform data and transparency in recommender systems are essential for independent scrutiny and democratic oversight.
- Moving forward, integrated enforcement and sustained research capacity – including cross-platform investigations and algorithmic audits – are vital to bridge the gap between regulation and evidence, ensuring a more transparent, accountable, and rights-based digital ecosystem in Europe. At the same time, these frameworks should remain proportionate and grounded in fundamental rights, supporting innovation while ensuring that systemic risk mitigation measures are applied responsibly and without unnecessary restrictions on freedom of expression.

INTRODUCTION

Technological development has created online spaces that barely existed a few years ago – platforms, websites, and apps that we now use to communicate, shop, learn, and express ourselves. The words that we use to describe these digital environments influence how we behave within them, yet we often depend on terms and systems we only partly understand. For example, algorithms quietly decide what news we see, which friends' posts appear first, or which videos we are encouraged to watch, shaping our sense of reality without us even noticing.

Social media brought terms such as "algorithm" and "algorithmic amplification" into everyday conversation. These terms are now used constantly, yet they are rarely defined with precision. Most people have only a partial understanding of how algorithms operate or how algorithmic amplification occurs. This terminology is ubiquitous in discussions about our digital environment, yet its substance often remains unclear.

This report, produced by EU DisinfoLab for the Friedrich Naumann Foundation for Freedom, aims to clarify what algorithms are, how they shape our digital experiences on social media platforms through their power to amplify and give visibility to certain content while de-amplifying others, and ultimately, why they matter to understand our digital ecosystems.

The first section provides a theoretical framework for algorithmic amplification, bringing together perspectives from academia, civil society organisations, private companies, and social media platforms. These perspectives are largely based on observation and inference, as there is no full visibility into how algorithmic amplification works. The lack of a universal definition reflects platforms' unwillingness to define or disclose these mechanisms, underscoring that the field is still a black box marked by a profound lack of transparency.

This opacity has significant repercussions on our digital lives and may even ultimately constitute a violation of EU legislation such as the European Digital Services Act (DSA).

The second section focuses on the pursuit of greater transparency and accountability in Germany regarding how platforms design and deploy their algorithms. Various initiatives led by German organisations illustrate ongoing efforts to better understand algorithmic amplification on social media platforms and to counter its malicious or self-serving use for political or economic purposes.

PART I – CONCEPTUAL OVERVIEW: DEFINING ALGORITHMIC AMPLIFICATION

While the concept of "algorithm" has broadly accepted definitions, there is far less consensus around its most salient effect in today's digital environment, namely algorithmic amplification. To inform this report, we gathered perspectives from across the field – academia, civil society organisations studying the issue, and, crucially, some insights into how digital platforms operationalise it. Our aim is to present a diverse theoretical lens on a phenomenon that lacks a universal definition and remains untransparent and poorly documented, despite its central role in shaping online experiences and behaviours. The existing understanding revolves around mechanisms such as recommender systems and content visibility. Since algorithms are opaque and formal definitions absent, much of the discourse relies on observation, inference, and some degree of speculation.

1. ALGORITHMS, ALGORITHMIC AMPLIFICATION, AND THEIR RELEVANCE IN OUR DIGITAL ENVIRONMENT

The Stanford Graduate School of Business offers a straightforward definition of an algorithm as "a replicable step-by-step process to accomplish a task", highlighting that algorithms are not limited to computers and programmers, but apply to any replicable routine in daily lives.

When applied to computers, the concept is technically well-defined as a "precise step-by-step plan" or "a finite set of unambiguous instructions" that takes input(s), performs a sequence of operations, and produces output(s). Even as complexity increases – requiring specific instructions for every potential path within a process – definitions still imply a clear, deterministic logic, a cause-and-effect structure typical of "a computational procedure".

Paradoxically, once they are embedded in digital ecosystems (from social media platforms to search engines, among others), that linearity becomes hard to trace. In these contexts, algorithms determine what users see and in which order, yet the logic behind those choices remains inaccessible outside the company's black box.

In such settings, **the focus often shifts from algorithms themselves to algorithmic amplification – the process by which algorithmic systems selectively elevate the visibility, reach, or spread of certain content**. Except for limited proprietary data available (e.g., Frances Haugen blowing the whistle on Facebook in 2021), most criteria guiding amplification – such as engagement, virality, user preference, or exposure patterns – can only be inferred.

Crucially, amplification is not itself a type of algorithm but rather a consequence or function of how an algorithm operates. Unlike "algorithm", however, "amplification" has no standardised definition. Each platform applies its own evolving logic for curation and ranking – an ever-changing "recipe" with largely undisclosed ingredients.

2. PERSPECTIVES FROM ACADEMIA

Academics have approached this question through multiple studies. This section spotlights four of them to examine how they conceptualise the phenomenon and identify the main components identified in platforms' algorithmic architecture.

POPULARITY, ENGAGEMENT, AND LIMITED USER AGENCY

[Annabell, T., et al. (2025). *TikTok Search Recommendations: Governance and Research Challenges.* arXiv preprint arXiv:2505.08385v1. https://doi.org/10.48550/arXiv.2505.08385]

This study focuses on TikTok's search recommendation feature – specifically, the pre-formulated search terms appearing in the homepage search bar and as overlays on videos. It examines how these recommendations are generated and moderated, revealing significant opacity in both processes.

Although the authors do not explicitly use the term "algorithmic amplification", they discuss **algorithmic curation in relation to moderation**. They identify relevance and engagement as key factors shaping which recommendations appear: **content popularity and prior user feedback** play crucial roles in determining visibility. Importantly, the authors also note that users have limited agency in this process, with no option to disable such recommendations.

TIME IS KING

[Bauman, F., et al. (2025). *Dynamics of Algorithmic Content Amplification on TikTok.* arXiv preprint arXiv:2503.20231v1. https://doi.org/10.48550/arXiv.2503.20231]

This study also examines TikTok – described by the authors as "an extreme case of an algorithm-driven ecosystem" – but focused on the For You Page (FYP). Rather than using the term "algorithm amplification", they define **content amplification** as the process by which the FYP increasingly shows users content that aligns with their interests the longer they scroll. As the feed adapts to individual interests, it progressively **narrows the range of recommendations**, showing less popular and more limited content.

They find that this **personalisation effect** emerges rapidly, often within the first 200 videos (about 1.5 hours). Although they note that the "dynamics of content amplification on TikTok remain largely unquantified",

the findings suggest that algorithmic amplification is shaped by **user interests and content popularity**, but primarily driven by **time spent on the platform**.

IT'S COMPLICATED… AND SYSTEMIC

[Lum, K., & Lazovich, T. (2023). *The Myth of the Algorithm: A System-Level View of Algorithmic Amplification.* Knight First Amendment Institute at Columbia University. https://knightcolumbia.org/content/the-myth-of-the-algorithm-a-system-level-view-of-algorithmic-amplification]

Produced as part of Columbia University's project on algorithmic amplification, this essay offers a working definition: "algorithmic systems can increase the reach of certain types of content", but amplification cannot be claimed without a comparison "relative to the reach they would have gotten under some other **neutral baseline**". The concept recognises the external and artificial capacity to amplify content exposure beyond its natural reach, implying potential disproportion or unfairness. Yet the authors question the very notion of neutrality, noting that even the baseline is shaped by multiple factors within a complex system.

They present algorithmic amplification as the outcome of an interconnected system combining ranking models, auxiliary models, manual components, and other elements – a **multi-level structure** whose parts influence one another. Ultimately, "the algorithm" is understood as the entire system. The authors propose more precise terms for related issues: "**algorithmic exposure**," for greater visibility of harmful content, and "**algorithmic inequality**," for imbalances and unfair treatment.

AN INSTRUMENT OF POWER

[Shad, K. B. (2025). *Algorithmic Hegemony: AI, Political Elites, and the Reinvention of Electoral Influence. Journal of Sociocybernetics, 20*(1), 13–41. https://doi.org/10.26754/ojs_jos/jos.2025111599]

Focusing on X, this article moves beyond algorithmic amplification to introduce the concept of **algorithmic hegemony**. Although it does not dissect the drivers of amplification in depth, it underscores how platforms tend to **reinforce content with high engagement potential** – typically emotionally charged, fear-based, and conspiratorial material.

The study's major contribution is its argument that algorithmic amplification has transformed platforms into an **instrument of power**. Engagement-driven algorithms, it contends, no longer simply mediate communication but govern democratic discourse and "co-create social and political realities". Platforms have shifted from "neutral conduits for information exchange" to sociopolitical agents. This embedded power dynamic, rooted in

platform design, risks eroding democratic deliberation and reinforcing new forms of authority that challenge traditional checks and balances.

3. PERSPECTIVES FROM CIVIL SOCIETY

It is not only academics who are seeking to understand algorithmic amplification. Civil society organisations (CSOs) working on digital rights and transparency have also been very active in this field. This section compiles the views of two leading organisations specialising in algorithmic research.

AIFORENSICS: ALGORITHMIC AMPLIFICATION AS AN EDITORIAL FUNCTION

AIForensics is a European non-profit that investigates influential and opaque algorithms. It holds "major technology platforms accountable by conducting independent and high-profile technical investigations to uncover and expose the harms caused by their algorithms".

The organisation does not have a formal definition of algorithm amplification, but its director and co-founder, Marc Faddoul, describes it as **the "editorial function" of a platform pursuing "engagement maximisation"**. This often means rewarding content that is attention-grabbing, financially rewarding, or new. He also points to some underlying mechanisms – such as user interactions, content recency, and geo-specificity – which mirror certain principles found in journalism.

"Algorithmic amplification describes the mechanisms through which platforms can increase (or decrease) the visibility of the content through algorithmic recommendations. It captures the '**editorial function**' **of the platform's algorithm** by virtue of being able to promote or demote certain pieces of content, akin to how a media editor can highlight specific stories on its front page. In that sense, it should engage the responsibility of the platform more directly than when simply hosting content," explains Faddoul.

"The most relevant dynamic that describes algorithmic amplification is the underlying optimisation goal of the algorithm, the main component of which is typically **'engagement maximisation'**. As such, the most engaging content tends to be disproportionately amplified, which creates a bias towards polarising or sensationalist content. There are also other secondary optimisation goals, such as favouring monetisable content or ensuring some level of novelty in the feed (to keep users engaged in the long run). Many features are leveraged in order to maximise this optimization goal, including features capturing the user's interactions with previous content, and others that characterise the specific piece of content. The recency and geo-specificity of the content are also given substantial weight", adds the expert.

ALGORITHMWATCH

AlgorithmWatch is a non-governmental, non-profit organisation based in Berlin and Zurich. According to its own definition, it fights "for a world where algorithms and Artificial Intelligence (AI) do not weaken justice, human rights, democracy, and sustainability but strengthen them".

Oliver Marsch, Head of Tech Research at the organisation, provides an insightful differentiation between the **amplification resulting from the "logic of the algorithm" and "disproportionately" high levels of visibility relative to a baseline expected from that logic**, and refers to the latter concept as the most relevant when studying the phenomenon.

In the first case, algorithmic amplification means that "specific content, accounts or decision outcomes receive high levels of visibility, engagement or importance by following the logic of the system, even if the outcome is not desirable in a holistic sense". In this case, polarising content posted by political actors could have more visibility because the algorithm "reads" the greater engagement received by this content or the politicians' high number of followers. Another example fitting in this case would be a hiring system prioritising men in recruitment, following the logic of an algorithm that rewards the existing workforce, which is disproportionately male. "The algorithms **follow the logic that platforms and providers have set out**."

In the second case, however, "a piece of content, an account, or a decision outcome receives **disproportionately high levels of visibility, engagement, or importance, relative to the baseline that one would usually expect such content to receive**. In this case, the difference could be explained by some **particular factor in algorithmic decision-making being deliberately tweaked or used specifically to boost visibility**, engagement, or importance". Hypothetical examples of algorithmic amplification might be a CEO instructing that their own content, or that of a particular party or ideology, receive additional visibility; botnets deliberately boosting engagement in defined geographies and causing that content to be labelled as "trending" in that area; or actors artificially tricking the algorithm by adding certain words or paying for views or engagement metrics.

4. PERSPECTIVES FROM PLATFORMS

Having clarified the definitions, we now turn to how some of the main social media platforms deploy algorithmic amplification in practice. Each platform operates through its own algorithmic architecture, shaped by business models, user behaviour data, and specific engagement goals.

- YouTube pioneered algorithms optimised for watch time, encouraging binge consumption through endless autoplay and, over time, more extreme or sensational recommendations.

- Google introduced the notion of the "filter bubble", personalising search results based on users' past behaviour and thereby limiting the diversity of information they encounter.
- Facebook was not the first to use algorithms, but it has mainstreamed the idea of the algorithmically curated feed since 2006. Meta later expanded this model to Instagram, where each feature – Feed, Stories, Explore, and others – relies on its own algorithm logic.
- TikTok has arguably set the new benchmark for algorithmic engagement. Its For You Page, now widely imitated by Meta and others, captures user attention through hyper-personalisation – learning from even minimal signals such as watch duration, replays, or pauses. The platform does not merely reflect user preferences; it actively shapes them, making its recommendation system both powerful and obscure.

5. ALGORITHMIC AMPLIFICATION AS A SYSTEMIC RISK

Algorithmic amplification has far-reaching repercussions. It can heighten users' exposure to disinformation and malicious campaigns, bias visibility toward certain political viewpoints, and create economic disparities, as platform visibility increasingly mediates access to income and opportunity.

In the study of disinformation, algorithmic amplification is a critical concept because it helps explain why false or misleading narratives gain disproportionate reach and influence online. Triggering, polarising, and often inaccurate content travels faster and farther across platforms, as negative and emotive stimuli elicit stronger reactions – signals that algorithms are designed to reward. Malign actors also exploit these mechanisms, for instance, through Coordinated Inauthentic Behaviour, strategically manipulating platform dynamics to amplify their content.

Recommender systems further reinforce this pattern by prioritising inflammatory or sensational material that generates engagement. While disinformation may originate from multiple sources, it is these engagement-optimised algorithmic systems that often propel such narratives into mainstream visibility, shifting the debate from free speech to free reach. Therefore, the challenge is to tackle these amplification dynamics in ways that protect free expression while reducing distortions, focusing on transparency, user choice and systemic risk mitigation rather than expanding the already considerable discretion that platforms can exercise over lawful content. These consequences are amplified by opacity. As discussed earlier, amplification systems remain a black box: without access to the full "recipe", researchers can only infer some of the ingredients and their interrelations.

In this context, algorithmic amplification itself, as an integral part of platform design, constitutes a systemic risk, as defined in Articles 34 and 35 and Recital 79 of the EU's Digital Services Act (DSA). It can also exacerbate other risks, including the spread of illegal content and the erosion of fundamental rights and democratic processes. Under the DSA, Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) must assess and mitigate "the systemic risks stemming from the design, functioning, and use of their services." Understanding algorithmic amplification is therefore essential to ensuring greater transparency and accountability in platform governance.

PART II – CASE STUDIES: LEGAL ACTION FOR ALGORITHMIC ACCOUNTABILITY IN GERMANY

The second section grounds the discussion in practice by examining Germany's recent legal and regulatory efforts to hold major platforms accountable. It brings together four emblematic cases that, in different ways, probe the inner workings of algorithmic systems – from recommender design and data access to market control and tracking infrastructures. Together, these lawsuits illustrate how Germany has emerged as a testing ground for enforcing transparency and accountability in algorithmic amplification.

While their legal bases and outcomes vary, spanning the Digital Services Act, GDPR, AI Act, and competition law, they share a common goal: to expose how platform architectures shape visibility, influence user behaviour, and impact democratic processes. Their collective importance lies in the willingness to challenge opacity, ask how algorithms amplify or suppress information, and push for frameworks that make digital power both measurable and accountable.

1. GERMANY IMPOSES X ACCESS TO DATA (AND THUS ALGORITHMIC TRANSPARENCY)

OVERVIEW

In early February 2025, two Berlin-based civil society organisations – Democracy Reporting International (DRI) and Gesellschaft für Freiheitsrechte (GFF) – sued X under the Digital Services Act (DSA), demanding access to the platform's publicly-available data (likes, shares, reach, real-time engagement) ahead of Germany's federal election. On 6 February 2025, the Regional Court of Berlin (Landgericht Berlin) issued an injunction ordering X to provide access to publicly available data until at least after the election period. X challenged the decision claiming that the German court lacked jurisdiction as the platform is headquartered in Ireland. In May 2025, the Court found that DRI was entitled to bring its claim in Germany, establishing a significant precedent by confirming that EU national courts may hold platforms accountable for non-compliance with data-access duties. While the case primarily concerns data access under the DSA, it can also be viewed as a step toward greater algorithmic transparency – enabling scrutiny of recommender systems and potential amplification mechanisms that shape political visibility online.

LEGAL BASIS

Under the Digital Services Act (Article 40(12)), Very Large Online Platforms (VLOPs) such as X must grant researchers access "without undue delay" to publicly-available data for research into systemic risks, including election influence. The provision is central to understanding how algorithmic amplification mechanisms – driven by ranking, recommendation, and virality features – might distort information flows during sensitive democratic processes like elections.

CONSIDERATIONS ON ALGORITHMIC AMPLIFICATION, DATA ACCESS, AND RESEARCH TRANSPARENCY

The German court's ruling against X goes beyond a procedural question of transparency: though centred on data access, it ultimately relates to understanding how the platform's systems operate, particularly how its design and recommender mechanisms may influence the visibility and spread of information.

The data requested by researchers – metrics such as likes, shares, reach, and engagement – form the **raw material of amplification** and may help better understand how platform propagation loops work. These indicators are the **inputs that recommender and ranking systems use to decide which content is surfaced, prioritised, or hidden**. Without access to this data, it is impossible to trace how visibility is distributed across political content or to identify when particular narratives are being algorithmically boosted or suppressed. These insights are essential for "detecting, identifying, and understanding systemic risks in the Union pursuant to Article 34(1)", including those linked to election interference.

By granting access to data, the court's decision indirectly addresses algorithmic exposure, enabling scrutiny on how content is amplified across the platform. Although the lawsuit does not centre on algorithms, **analysing engagement surges, echo chamber dynamics, or virality patterns in the released data would provide valuable insight into how these algorithm-led processes operate**. The decision also reinforces a broader principle of research transparency and democratic accountability: platforms whose algorithms shape political communication must be open to independent examination. Without data access, recommender systems remain opaque – black boxes capable of influencing civic discourse and affecting elections integrity without external oversight or accountability. Ultimately, the legal foundation lies in the Digital Services Act's data access provisions, but the **deeper significance concerns democratic governance of algorithmic power**.

2. GERMANY LAUNCHES CLASS ACTIONS OVER TIKTOK AND X'S RECOMMENDATION ALGORITHMS

OVERVIEW

On 5 February 2025, the Dutch consumer foundation SOMI filed four cross-border class actions in Germany against TikTok and X, represented by German law firm Spirit Legal. The lawsuit claims that the platforms have broken multiple EU and German laws, asking the companies to stop these practices and pay compensation worth several billion euros. Germany's Federal Office of Justice has since added that TikTok case to the official register for collective lawsuits, which allows users and small businesses to join the action. According to SOMI and Spirit Legal, TikTok and X **unlawfully process personal (including sensitive and minors') data and deploy manipulative, addictive product designs that fuel recommendation algorithms**. The filings position the cases as early tests of the DSA, GDPR, and the AI Act.

LEGAL BASIS

Under the General Data Protection Regulation (GDPR), the claimants argue that TikTok and X process users' personal data unlawfully. They allege that the platforms rely on invalid consent mechanisms, handle sensitive categories of data without a proper legal basis, profile minors, and fail to meet basic GDPR principles such as transparency, purpose limitation, and data minimisation.

Under the Digital Services Act (DSA), the suits claim that both platforms breach their duties to **assess and mitigate systemic risks, including those related to election integrity and the protection of minors**. They also accuse TikTok and X of failing to grant researchers sufficient access to data that would allow **independent scrutiny of how their recommender systems operate**. The complaints frame these shortcomings within Articles 34–35, which deal with risk management and transparency obligations for Very Large Online Platforms (VLOPs).

Finally, under the forthcoming EU Artificial Intelligence Act (AI Act), the plaintiffs argue that **certain AI-driven features, such as recommendation and profiling systems, fall within the Act's requirements on risk management and transparency**. They present these mechanisms as high-impact AI systems that should be governed to prevent manipulation and ensure accountability – especially where they influence minors or public debate. Courts will need to clarify how these provisions apply as the AI Act gradually comes into force.

CONSIDERATIONS ON ALGORITHMIC AMPLIFICATION, MANIPULATIVE DESIGN, AND DATA-DRIVEN RECOMMENDERS

At the centre of these class actions is the claim that TikTok manipulates young users, feeding its recommendation algorithms with sensitive data, and that X uses sensitive data without a valid legal basis to power its algorithm. In short, unlawful data collection and processing fuels opaque recommender systems that determine which voices and narratives are amplified online.

EU rules provide different tools to tackle how data misuse feeds algorithmic amplification. Under the DSA, VLOPs must give users control over their recommenders work (Article 27), and identify, assess, and reduce systemic risks (Articles 34-35) such as threats to civic discourse, elections, and minors. The DSA's goal is to reveal what signals drive amplification, offer non-profiling options, and require platforms to reduce risks when ranking choices create visibility asymmetries or promote harmful content. This logic is echoed in recent EU election guidelines, which explicitly connect recommender design to systemic risk and outline mitigation expectations.

The GDPR sets the standards for lawful processing and transparency. If recommendation systems rely on sensitive data (like inferred political views) or on profiling minors, platforms face strict legal thresholds. Therefore, GDPR compliance is a precondition for any legitimate amplification architecture. Then, the EU AI Act adds another governance layer by banning manipulative AI practices. Article 5 prohibits recommender systems that use addictive or deceptive design – such as nudges exploiting users' emotions, habits, or vulnerabilities to keep them engaged – and subjects platforms to risk-management duties when their design choices covertly influence user behaviour. Together, these three laws create a complementary framework for making algorithmic systems safer and more accountable.

The complaints describe a common pattern: tracking and profiling feed ranking algorithms that optimise for watch time, clicks, or shares. **When these systems use sensitive traits or child data, they can amplify attention-grabbing content –such as disinformation, deepfakes, or polarising material** – while filtering out alternative views. This produces visibility gaps that users cannot detect or challenge, resulting in two-fold harms: systemic risks to democracy and child-specific harms (e.g., addictive use, pressure to engage, and mental-health effects). Such trends are in line with European Parliament findings, which highlighted TikTok's risk profile around addictive design, data practices, and election-related harms, underscoring the policy context into which these suits land.

Ultimately, these lawsuits ask more than whether TikTok and X broke privacy or platform rules. They question the very design of their recommender systems – whether the data they use and the behaviours they optimise for are lawful, fair, and safe. Moreover, they show how this trio of EU regulations work in a complementary way

and point toward a unified remedy: making algorithms auditable, transparent, and accountable to both users and democratic oversight.

3. GERMANY CHALLENGES AMAZON'S ALGORITHMIC PRICING POWER

OVERVIEW

In June 2025, Germany's antitrust authority (Bundeskartellamt, FCO) issued a preliminary legal assessment finding that Amazon's price-control mechanisms likely breach national and EU competition law. The authority argues that the platform monitors sellers' prices – both on its marketplace and elsewhere (i.e., other e-commerce platforms, retailers' own webshops, and online price-comparison sites) – using automated checks and algorithmic enforcement. In practice, **when prices fall outside Amazon's acceptable range – whether too high or too low –affected listings may lose visibility, advertising eligibility, or even be removed**. According to the FCO, this practice restricts sellers' pricing freedom and limits competition both on and beyond Amazon's platform.

LEGAL BASIS

Under German special abuse control (Section 19a(2) of the German Competition law), companies with exceptional market power face stricter rules against self-preferencing (i.e., giving unfair advantage to their own products or services) and exploitative or exclusionary practices. In 2022, Amazon was officially classified as one of these companies, meaning it must not use its dominance to disadvantage others, and the German Federal Court of Justice later confirmed this status. In June 2025, the competition authority said Amazon's price controls may break this rule by unfairly limiting how sellers set their prices.

Under EU law (Article 102 TFEU) and Germany's general abuse rules (Section 19 GWB), powerful companies must not misuse their dominance. The competition authority implies that Amazon may have broken these rules by using its control over the marketplace to influence sellers' prices and limit their access or visibility on the platform.

CONSIDERATIONS ON ALGORITHMIC AMPLIFICATION, MARKET RANKING POWER, AND PRICING SYSTEMS

The FCO's investigation places Amazon's algorithmic systems – particularly its automated price-checking and ranking mechanisms – at the core of the suspected abuse. These systems operationalise Amazon's notion of price fairness by constantly comparing listed prices against those on other websites. **If a seller's offer is judged too expensive, Amazon's algorithms can downgrade its visibility**, remove it from advertising

slots, or even exclude it from the Buy Box (the default purchase option). Conversely, **offers that fit Amazon's internal thresholds are amplified** – they appear higher in search results, are more likely to win the Buy Box, and are prominently featured in recommendations.

This dynamic of algorithmic amplification and suppression means the system does not just reward competitive pricing, but it actively penalises deviation. The two sides of the same mechanism reinforce one another: amplification of compliant sellers magnifies suppression of others, effectively shaping both supply and demand. Because **the recommendation criteria are opaque and automated**, sellers cannot predict or contest how their listings are treated. The FCO views this as a non-transparent governance model that strengthens Amazon's control over pricing and market visibility, creating a dependency effect where sellers must conform to Amazon's algorithmic expectations to remain commercially viable.

According to the platform, its algorithms are designed to optimise efficiency and protect consumers from uncompetitive prices. Many merchants report that they cannot set independent prices – even on their own websites – without risking loss of visibility on Amazon. This creates a different effect on discounting elsewhere, as sellers align their broader pricing strategies with Amazon's algorithmic thresholds. Over time, this may reduce price diversity across the e-commerce ecosystem, entrenching Amazon as the de facto arbiter of what counts as a fair price.

While the FCO's case is legally framed around abuse of dominance, the same algorithmic mechanisms can harm consumers in several indirect ways. For instance, it may lead to higher prices overall, not because Amazon rewards expensive listings, but because sellers align their broader pricing strategies to avoid algorithmic penalties. In practice, many stop discounting on their own sites or rival platforms to avoid algorithmic penalties, which reduces price competition and lifts market-wide price levels over time. Moreover, it may reduce choice as listings above a certain threshold are hidden or removed, so consumers see a narrower range of offers and often miss higher-quality, niche, or sustainably produced products. Finally, **there is an issue of algorithmic steering as recommender systems control what users see**, pushing them toward what the algorithm defines as fair or convenient. Yet, these evaluations reflect the platform's commercial logic rather than the user's preferences. Therefore, the FCO frames these mechanisms as **a structural form of market control achieved through algorithmic conformity**.

4. GERMANY FINES META OVER UNLAWFUL TRACKING PRACTICES

OVERVIEW

In July 2025, the Regional Court of Leipzig ruled that Meta Platforms, Inc. violated the General Data Protection Regulation (GDPR) by using tracking technologies – namely Meta Pixel and software development kits (SDKs) – embedded across third-party websites and apps. These tools collected extensive user data, including from individuals not logged in to Facebook or Instagram, and transmitted it to Meta without a valid legal basis. The court found that the combination of technical identifiers and behavioural data allowed Meta to personally identify and profile users, breaching EU privacy law. This ruling fits into a broader regulatory push across Europe to limit cross-site tracking and data aggregation that feed large-scale profiling systems.

LEGAL BASIS

The court's decision rests on Articles 6 and 9 of the GDPR, which require a lawful basis and explicit consent for processing personal or special-category data. Meta's use of tracking systems was found to exceed these limits as users were tracked across domains without informed consent. Additionally, data from logged-out or non-Meta users was still collected and linked to unique identifiers. The purpose of optimising ads and measuring conversions did not meet GDPR standards of necessity and proportionality.

CONSIDERATIONS ON ALGORITHMIC AMPLIFICATION, DATA PROFILING, AND TARGETED RECOMMENDER SYSTEMS

Although the case primarily concerns data protection, it has clear implications for algorithmic transparency and amplification. Tracking technologies like Meta Pixel create the data infrastructure that fuels algorithmic recommendation, advertising, and ranking systems. Each data point – what users view, click, or abandon – feeds the models that determine which content or ads appear, to whom, and how often.

By ruling against Meta's data-collection methods, the court indirectly challenges the inputs that drive amplification. **Without such profiling data, algorithms have less capacity to microtarget or prioritise content based on inferred emotions or preferences**. In this sense, the decision acts on the foundation layer of algorithmic amplification, even though it does not address recommender bias or content visibility directly.

At the same time, the judgment highlights **a persistent opacity problem: users and regulators still lack visibility into how collected behavioural data is transformed into algorithmic outputs**. By curbing unlawful cross-site tracking, the ruling reinforces the principle that algorithmic influence begins with data

governance and that privacy enforcement is an essential step toward accountability for how recommender systems shape visibility and behaviour. Strong data-protection safeguards have long been understood as a precondition for digital freedom: users must be able to understand and control when and how their data fuel algorithmic profiling, especially when those profiles drive amplification and targeting that remain largely invisible to them.

CONCLUSIONS, LESSONS LEARNT, AND WAYS FORWARD

Germany's experience provides a valuable testing ground for understanding how algorithmic amplification intersects with law, governance, and democratic accountability. The country's recent lawsuits and regulatory actions illustrate both the potential and the limitations of national-level enforcement in addressing systemic risks emerging from opaque algorithmic systems.

1. DATA ACCESS AS A CORNERSTONE OF ACCOUNTABILITY

The case brought by DRI and GFF against X under the DSA marked a significant step toward operationalising platform transparency. By ordering X to grant access to publicly available data, the Berlin court strengthened researchers' ability to analyse algorithmic dynamics in real time, particularly around elections. Access to data such as engagement, reach, and impressions enables independent scrutiny of amplification patterns, which is an essential step in detecting biases and systemic risks in recommender systems. This approach reflects growing recognition that data transparency is not just a procedural right but a precondition for democratic oversight and accountability in algorithmic governance.

2. ALGORITHMIC AMPLIFICATION AS A SYSTEMIC RISK

Across these cases, algorithmic amplification emerges not only as a technical or ethical issue but as a systemic risk under the DSA framework – as an integral part of platform design capable of distorting political visibility, polarising discourse, and influencing democratic processes. The German experience shows that when amplification mechanisms reward engagement and outrage, they can indirectly shape election debates and public trust in institutions. This confirms that understanding and mitigating algorithmic amplification is integral to safeguarding information integrity and civic resilience.

3. THE ROLE OF RESEARCH AND INDEPENDENT AUDITS

Civil society and independent researchers play a pivotal role in unpacking these dynamics. Projects such as CrossOver demonstrate how cross-platform monitoring can expose how recommender systems amplify disinformation, polarising content, and malicious campaigns. These efforts underscore the value of adversarial research, algorithmic audits, and technical experimentation in complementing legal and regulatory action. Continued EU and national funding, along with structured data access frameworks, are essential to bridge the

current gap between policy ambition and empirical evidence, enabling a more transparent and accountable algorithmic ecosystem.

4. EXPANDING THE SCOPE TO AI REGULATION

Germany's recent lawsuits show that algorithmic amplification cuts across multiple policy areas – data protection, competition, and AI regulation. The four cases examined illustrate this interconnection: the DSA lawsuit against X centres on data access for transparency; the class actions against TikTok and X expose how engagement-optimised design amplifies manipulative or harmful content; and the Amazon case shows how algorithmic ranking shapes market visibility and pricing power.

Together, they reveal that amplification is driven by the same data and machine-learning infrastructures underpinning large-scale AI systems. These are not the only ongoing proceedings: another German lawsuit, targeting Meta's AI training on personal data, further illustrates how unlawful data collection fuels amplification and profiling. Addressing these risks requires integrated, proportionate enforcement across the DSA, GDPR, AI Act, and competition law, ensuring that algorithmic design, data governance, and AI accountability are treated as inseparable components of platform regulation.

5. OVERLAPPING LEGAL FRAMEWORKS AND SHARED COMPETENCE

Germany's actions illustrate how the DSA, GDPR, and AI Act form a mutually reinforcing framework for algorithmic accountability, each addressing different aspects of transparency, data protection, and risk management. In practice, however, the intersection of these frameworks also exposes persistent questions of **competence, coordination, and enforcement across jurisdictions**. **While algorithmic governance is largely defined at the European level, enforcement often depends on national authorities, courts, and regulatory agencies**. The German cases show how national actors can act as early enforcers, testing EU law in concrete contexts, influencing regulatory interpretation, and setting precedents that will shape future understandings of systemic risk, algorithmic responsibility, and digital governance across the Union.

6. LESSONS MOVING FORWARD

Germany's experience offers several lessons for strengthening EU-level oversight of algorithmic systems.

- Transparency starts with data access. Without it, research, auditing, and accountability remain impossible.

- Algorithmic amplification should be treated as a systemic risk in its own right, especially during elections or moments of crisis.
- Independent research needs long-term institutional support, so that evidence, not speculation, guides regulation.
- AI governance and data protection must be integrated into discussions on amplification, since they all rely on the same infrastructures of profiling, optimisation, and influence.
- National enforcement remains essential, not as a sign of fragmentation but as a form of experimentation that strengthens the EU's collective regulatory capacity.
- This path must also safeguard freedom of expression, media pluralism, and entrepreneurial freedom, aligning transparency and accountability measures with democratic values and the integrity of public debate.

Ultimately, Germany's legal and civic efforts show that holding platforms accountable requires a **whole-of-system approach: transparency of inputs (data), explainability of processes (algorithms), and accountability for outcomes (amplification)**. Together, these elements define the path toward a safer, fairer, and more democratic digital ecosystem in Europe.