Allegations of Algorithmic Manipulation: France Opens Criminal Probe into Elon Musk's X

Infosources™

July 12, 2025

French prosecutors have launched a criminal investigation into X (formerly Twitter) over allegations of algorithmic manipulation and unauthorized data extraction. The probe, led by the J3 cybercrime unit, follows formal complaints from a French MP and a senior official who suspect that X's ranking systems were intentionally distorted to serve political interests and gather user data unlawfully.

The investigation focuses on two charges:

1. **Tampering with automated data systems as part of an organized group, and**
2. **Fraudulent extraction of data.**

The case raises broader concerns about foreign interference, algorithmic opacity, and compliance with EU digital laws, as X continues expanding into financial services within Europe.

The French justice system has entered new territory with a criminal investigation targeting **X** (formerly Twitter), focusing on allegations of algorithmic manipulation and foreign interference. The case—now in the hands of the country's elite cybercrime unit **J3**—signals a significant turning point in how Europe approaches the political and technical power wielded by social media platforms.

The probe follows complaints filed in January by French MP **Éric Bothorel** and a senior government official whose identity remains undisclosed. Bothorel, a member of President Emmanuel Macron's party, publicly stated that he believed the X platform had "extreme informational bias" aligned with the personal views of **Elon Musk**, made possible only through intentional algorithmic tampering.

💡

*Tampering refers to illegally interfering with how a computer system or algorithm works, and secretly **modified or steered** to:1-Prioritize certain political opinions over others.2-Hide or suppress opposing viewpoints.3-Promote disinformation to serve foreign political agendas. An internal engineer, for instance, working with an external political group intentionally adjusts algorithm weightings to make specific hashtags trend more often. This misleads users into thinking a certain political movement is gaining traction—when it's not.*

A New Legal Frontier: Algorithms Under Criminal Lens

According to a statement issued by magistrate **Laure Beccuau**, prosecutors are investigating two specific charges: (1) tampering with automated data processing systems as part of an organized group, and (2) the fraudulent extraction of data from such systems. Both offenses fall under French criminal statutes related to cybercrime and could carry serious penalties if proven.

💡

Fraudulent extraction of Data refers to stealing or improperly collecting data such as:
1-Harvesting detailed behavioral profiles (likes, views, scrolling habits).
2-Extracting metadata (location, device info) from people who didn't opt in.
3-Scraping conversations from private accounts or DMs using backdoors.
*If this data was later used to fuel targeted political manipulation, sold to third parties, or fed into foreign influence campaigns, it fits this charge. A coordinated group uses bots and fake accounts to interact with real users, collecting their reactions and engagement patterns. This data is then used to **build psychographic profiles** that can predict political behavior or susceptibility to propaganda.*

The **J3 cybercrime unit**, known for its high-level operations including the recent 2024 arrest of Telegram founder Pavel Durov, has officially taken over the investigation. Initial leads suggest the manipulation may not just be technical in nature but could be part of a broader strategy involving political influence campaigns, either foreign or domestic.

The Mechanisms Behind Algorithmic Manipulation

Although the French probe is still in its early stages, experts in digital forensics and algorithmic auditing have for years warned about the **opaque nature of ranking systems** on platforms like X. Algorithmic manipulation doesn't require visible censorship or overt messaging—it often happens in subtle ways that significantly shape user experience.
For example, recommender systems can be designed or adjusted to **boost specific ideological content**, giving it disproportionate reach compared to neutral or opposing viewpoints. This isn't necessarily accomplished through outright favoritism, but through tweaks in how the system defines "relevance" or "engagement."

💡

In such opaque nature of ranking systems users don't know how or why certain posts or accounts are ranked higher or lower, because the algorithm's inner logic is not made public. Opaque systems make it easy to: 1-Manipulate public opinion without people realizing.2-Hide bias or favoritism.3-Avoid accountability if the system is used unethically.
*That's why regulators, like the **EU under the Digital Services Act**, are pushing platforms to make ranking algorithms more **transparent** and **auditable**.*

In practical terms, such manipulation could look like:

- **Preference for engagement-rich content**: Political content that elicits more likes, shares, or outrage may be algorithmically promoted regardless of factual accuracy.
- **Echo chambers and filter bubbles**: The system learns from a user's behavior and gradually filters out conflicting information, reinforcing ideological bias.
- **Coordinated timing**: If certain tweets are strategically promoted or allowed to trend at key moments—such as during elections—this creates the illusion of organic public consensus.
- **Bot amplification**: Coordinated bot or troll activity can simulate interest in specific content, tricking the algorithm into further boosting it.
- **Data profiling**: Extracting behavioral data via the platform's backend allows deeper targeting of susceptible audiences, especially when combined with external datasets.

This manipulation can occur passively—built into the logic of profit-seeking engagement algorithms—or actively, if someone with access modifies ranking variables with intent.

X's History of Regulatory Clashes

The allegations are not without precedent. Since Elon Musk acquired X in 2022, the platform has repeatedly found itself at odds with regulators, especially in Europe. In February, X lost a case in the **Berlin Regional Court**, requiring it to hand over public engagement data to researchers studying electoral interference. Furthermore, the European Commission is currently investigating X under the **Digital Services Act (DSA)**—a landmark regulatory framework aimed at forcing transparency around how platforms manage content, including how algorithms rank, remove, or amplify it.

Musk, meanwhile, has announced ambitious plans to transform X into a **"financial super app"** anchored by crypto technologies and digital wallets. Yet these ongoing probes may cast a long shadow over those ambitions. Regulatory trust is essential to offer licensed financial services in the EU, and any suggestion that the platform is being used for political influence could be a dealbreaker for compliance.

A Broader Political and Ethical Crisis

What's striking in this case is that **algorithmic manipulation is no longer a theoretical concern**. Governments are now willing to pursue criminal investigations into the technical architecture of platforms when national integrity is at stake. The lines between tech design, editorial control, and foreign policy are becoming increasingly blurred.

Whether X is proven guilty of these allegations or not, the case raises urgent questions about the **limits of platform power** in democratic societies. Who gets to control the visibility of political narratives? What happens when ranking algorithms evolve from neutral tools into strategic levers? And more importantly, how can societies audit or counteract these manipulations when the code is proprietary, complex, and invisible to the public?

What Happens Next?

As of now, X has **declined to comment** on the investigation, citing concerns about "platform independence" and free speech. Meanwhile, France's J3 unit has begun requesting backend data and system logs to determine whether platform behavior can be traced to deliberate manipulation or systemic design flaws.

The outcome of this probe could set major precedents. If prosecutors find evidence of intent or collusion, it may lead to the **first criminal case** built entirely on how an algorithm operates. At the very least, it marks the growing willingness of democratic governments to demand accountability from private tech firms whose influence now rivals that of traditional institutions.