AI, Backlash, and Security

25 FEBRUARY 2026

Giovanni De Pellegrini



Backlash against new technologies is growing, and the risk of anti-technological sentiment becoming a major threat to security must be addressed by the EU.

The historical period we live in has seen a rise in opposition to technological evolution. We have seen attacks against 5G infrastructure at the outset of the Covid-19 pandemic, discontent towards the implementation of AI in multiple fields, like labor, ethical concerns regarding the use of such tools, and worries about the environmental impact of the infrastructure needed to support such advancements.

Underlining the evolution of such threats, on November 5, 2025, The Soufan Center stated it had identified a proliferation of physical threats against AI and the datacenters used to host and train it.

The topic of technology as a tool to pursue violent actions has been analyzed for years. The *EU Terrorism Situation and Trend Report 2025* by Europol underlined that the exploitation of new technologies by terrorists and extremists reached «unprecedented levels» in 2025. The report highlighted the use of generative AI at its apex to create and spread propaganda.

The current security situation in the EU puts awareness of the usage of new technologies for terrorist, extremist, and violent acts at the forefront of its security policies, but acknowledgement of the possibility of technology becoming the target, not the means, of violent acts is lacking.

While addressing the origins of disenfranchisement towards technology, an intersectional approach enables us to highlight different issues that anti-technological sentiment reveals.

Brian Merchant's *Blood in the Machine: The Origins of the Rebellion Against Big Tech* and Matteo Pasquinelli's *The Eye of the Master: A Social History of Artificial Intelligence* demonstrate the linkage between technological innovation and the replacement, or deconstruction, of labor. When thinking about machines substituting human work, one of the first examples that comes to mind is the Industrial Revolution and the Luddite movement. While defining Luddites as terrorists would represent an erroneous and grave framing of the movement from an ideological and historical point of view, their smashing of textile machinery during their protests in early XIX Century England represents one of the most famous acts of violence directed against technology. It shows resistance to change in labor driven by new technologies is not new, has happened before, and could happen again. In 2025, the adoption of AI by global organizations reached 78%, and almost 80.000 jobs were lost to AI the same year. Nartey's research shows «41% of global employers plan to reduce workforce due to AI automation within 5 years», increasing the number of people who could become disaffected by the phenomenon.

The second field influencing anti-technological backlash is the environment. Before the rise of AI, the technology of 5G sparked worries about environmental and human health effects during the first commercial rollout between 2019 and 2020. While these risks have been widely debunked, the first rollout saw numerous arson attacks against telecommunication towers, and at least in one case, technicians working on a tower were targeted by firearms. The backlash against 5G represented one of the newest fronts against technology, but pales in comparison to the backlash datacenters face. They represent a growing source of energy and water consumption, waste heat, and electronic waste. Numerous cases have been reported of communities hardly hit by negative effects after their construction in the area, such as skyrocketing energy prices, contaminated water sources due to residual waste, and excessive air pollution.

Lastly, several ethical concerns complete the framework of roots. Bias in large language models (LLMs), privacy and surveillance issues, and transparency and accountability are among the major ones that the evolution of AI models and their implementation in our everyday lives has brought forward in recent years. These issues remain somewhat difficult to frame efficiently, since the nature of the technology itself is one of continuous evolution. However, a common denominator can be identified: how both public and corporate policies address the existing and arising risks. Regulation becomes central to tackle these issues, and stakeholders and regulators can make a difference in public perception of new technologies. One of the latest examples comes from the United Kingdom, where the government threatened action against X, formerly known as Twitter, after a streak of sexually explicit deepfakes generated by various subscribers using the platform's generative AI, Grok. Elon Musk's response was to limit the use of Grok's AI image function to users who pay a monthly fee, while accusing the British government of looking for «any excuse for censorship».

To approach the risk of anti-technological extremism, two different viewpoints must be examined.

The first point involves security as a concept and the system that addresses it. The EU has a multi-level approach to terrorism and security. This includes institutional coordination, legal frameworks, operational entities, and cooperation with Member States. Since security levels are a national concern, the EU's role lies in supporting, coordinating, and harmonizing. This means the EU does not replace the Member States but rather works as a harmonizing entity.

Legal harmonization built institutionalized cooperation throughout the years, such as through Directive 2017/541 on combating terrorism, the main pillar on which one of the most critical aspects of security in the EU took form: advanced data-sharing systems. The Schengen Information System (SIS) represents the largest and most widely used information-sharing system for security and border management in Europe. A list of competent authorities that can directly access SIS's data is revised and updated every year. Further databases address other types of data. Travel and mobility intelligence is widely handled through the Passenger Name Record Directive (PNR), which mandates airlines to transfer passenger data for international flights to EU national authorities to combat terrorism and serious crime, allowing data analysis, risk assessment, and identification of suspects in a context of cross-border cooperation. Another example of security cooperation and integration is the European Criminal Records Information System – Third Country Nationals (ECRIS-TCN), a database facilitating the exchange of criminal records information of non-EU citizens across EU Member States.

One of the major strengths of the EU is the Brussels Effect, which refers to its ability to influence global standards and policies through regulation. However, at the end of 2025, debates began to appear on the validity of the

instrument to approach the continuously evolving world of new technologies and tech policy. The first sign of a shift towards the regulation process of new technologies in the EU first appeared as a rumor in November 2025, with the Commission proposing a pause to artificial intelligence laws. This then evolved into an omnibus, a legislative package grouping together several amendments to existing rules, «to a large corpus of digital legislation, selected to bring immediate relief to businesses, public administrations, and citizens alike, and to stimulate competitiveness». The move is reported to have taken place after heavy pressure from the U.S. government and American tech companies and is set to delay the enforcement of rules and requirements included in the AI Act and, as the Center for European Policy Analysis reported, retool the GDPR data protection law.

The decision to yield to Washington's insistence might open a Pandora's Box of anti-technological resentment, given the possibility that Brussels could abandon one of its main strengths, used over the years to safeguard its citizens, in favor of the will of a foreign power and its interests. After all, it must be remembered that the EU reports a variety of attitudes, both positive and negative, toward the implementation of AI and other new technologies among the citizens of its member states, as reported by the 2025 AI Index Report. Furthermore, a case where deregulation becomes the new policy does not help the EU to address backlash and disenfranchisement against new technologies, those that create them, and those who use them. What this decision does is leave ample margin to groups already seeing technology as a threat to pursue their goals with more liberty and traction. As an accelerated, more rapid evolution of technology and its applications takes hold, parts of societies across countries most impacted by the phenomenon could find themselves charmed by these groups and movements that promise to violently tackle the cause of their frustration towards technology. These groups, through their narratives, may try to explain people's struggles linked to technological evolution. An anti-technological narrative may be used to explain why someone's job was lost to AI, why their energy bills skyrocketed due to a datacenter's construction, or perhaps how to fight the perception that digital policies supposedly destined to better safeguard our society are in reality more comparable to a 1984's Big Brother scenario, where tech companies are far more able to influence legislation than the common citizen, but where it is the latter that takes a loss. In other words, in the case of anti-technological disenfranchisement, regulatory and policy issues are at risk of becoming security issues too.

Current EU instruments barely address the risk of anti-technological dissatisfaction.

In the case of tech policies, their focus has been, so far, attempting to push an agenda to bring Europe to the center of the race in the development of new technologies, particularly AI. At the same time, digital infrastructure, such as the one supporting cloud computing, has come under scrutiny as a new security matter, with the EU struggling to reach digital sovereignty.

While the risk of sabotage to infrastructure has taken priority in the more general security strategy the EU pursues, the possibility of these acts of sabotage taking place has usually been associated with actions by external actors.

While the risk of an escalation of anti-technological violence is currently considered low, to begin addressing it as a possible, factual threat, it would be necessary to understand that backlash dynamics on this matter can emerge at the intersection of regulation, social policy, and internal security. The problems deriving from the acceleration of technological evolution and the implementation of such tools are transversal and thus require an instrument that addresses this characteristic.

The proposed instrument is a transversal focus group that should be associated with the European Commission. It should take the form of a permanent focus group designed to address the multidimensional risks associated with the implementation of new technologies before they crystallize into social or security challenges.

The tool's value would lie not in coercive powers but in coordination, anticipation, and analytical capacity. By integrating different perspectives of governance, such as labor policy, environmental governance, and internal security, the instrument would be able to assess how policies related to new technologies interact in practice, rather than in isolation. This would improve anticipatory governance. The tool would be able to detect early symptoms of disenfranchisement by analyzing public discontent, the use of technology, and regulatory force together. Secondly, the transversal mechanism would promote policy coherence. Policies aimed at safeguarding basic rights and efficiency gains could contribute to feelings of exclusion if they fail to get matched with social or economic support strategies. The focus group might point out inconsistencies and contradictions by evaluating initiatives on new technologies in diverse policy areas, and thus help create balanced governance outcomes by considering these initiatives from different perspectives.