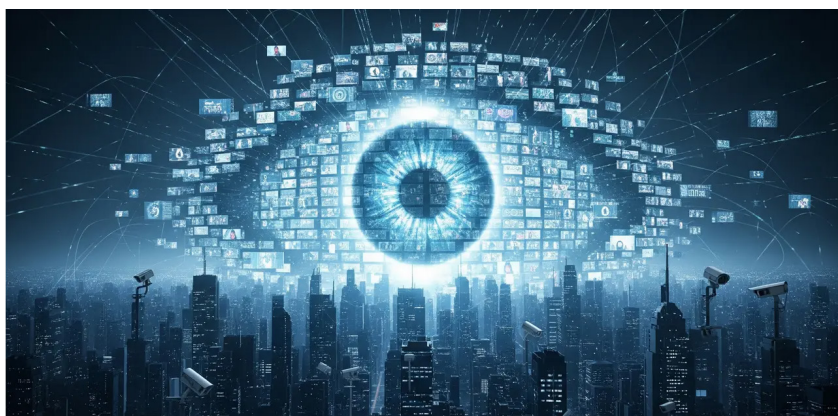


Data, democracy and the new art of war

Data is becoming the nervous system of the modern state. AI can help democracies govern better and fight smarter, but it can also turn public service into surveillance, as Sham Banerji reports.

6-minute read

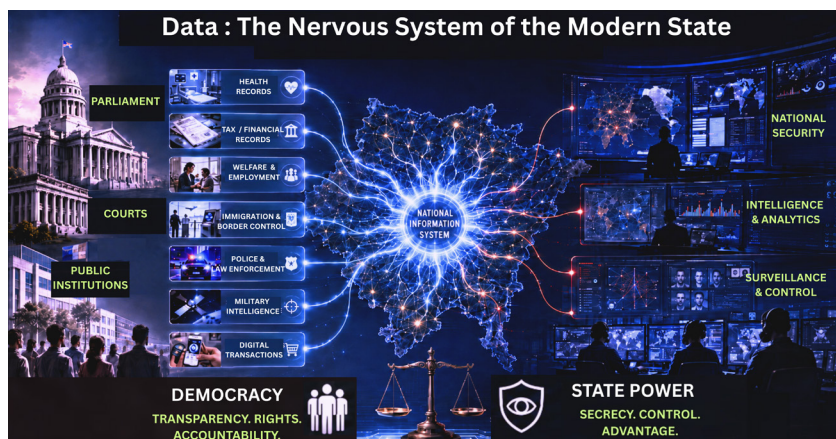


As governments and corporations gather unprecedented volumes of data, artificial intelligence is transforming information into a strategic source of political, economic and military power.

In the recent Vatican statement on the politics of AI, Pope Leo XIV argues that health, genetic and demographic data have become the new ‘rare earths’ of power. The pontiff warns that data is one of the central political resources of the AI age and should not be controlled by ‘a handful of actors’.

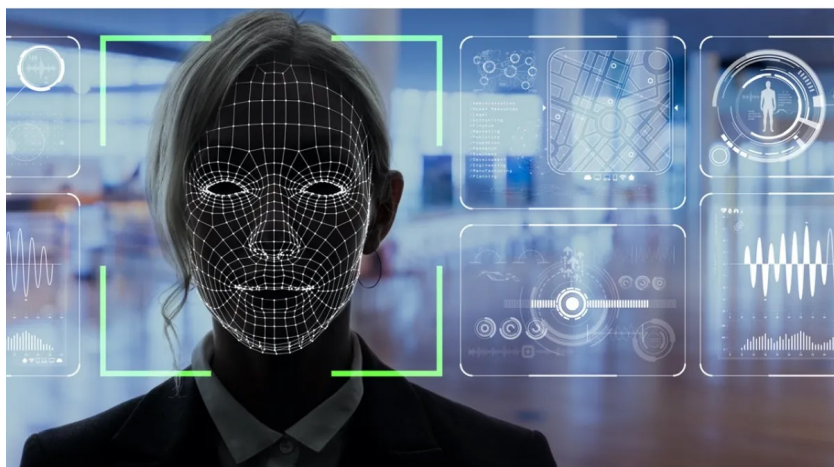
At the launch in May the only technologist on the Vatican’s panel of listed speakers was Christopher Olah, co-founder of Anthropic, who delivered an unusual confession from inside Big AI: ‘Every frontier AI lab, including Anthropic, operates inside a set of incentives and constraints that can sometimes conflict with doing the right thing’. He added that what was needed were ‘moral voices that the incentives cannot bend’.

For nations, raw data is no longer the main prize. A live, cross-linked information system, connecting health records, tax files, welfare claims, immigration data, police logs, satellite images and commercial transactions is far more valuable. Once linked by AI software, such systems can give governments powerful, actionable intelligence. This makes citizen data infrastructure as strategic as roads and electricity grids. Its architects are the new contractors of state power.



Modern governments increasingly link health, tax, welfare, security and financial information into integrated data systems that function as a digital nervous system.

The *Financial Times* reports that China is in the process of overhauling the world's largest surveillance network with advanced AI, giving the state powers to track people, analyse behaviour and predict potential unrest in real time. China's draft law on Cybercrime Prevention and Control, published by the Ministry of Public Security, remains at the draft stage after public consultation closed in March. The danger is not only surveillance after the fact, but prediction: systems designed to identify risk before any offence has taken place.



Advances in AI surveillance allow authorities to monitor behaviour patterns and identify perceived risks before any crime has been committed.

If enacted, it would consolidate telecoms, internet and banking rules into a single cybercrime framework. Hikvision, China's leader in smart-city surveillance and video analytics, and Huawei, the telecoms and AI chips giant, are expected to provide much of the physical architecture. Human-rights groups are quick to point out how mass surveillance systems, like the 'Integrated Joint Operations Platform' used in Xinjiang, can enable monitoring of minorities, punish 'untrustworthy' behaviour, restrict travel and deny services. They warn against behaviour-modelling software that assess risk or intent. The trigger for state action is not something the citizen has done. It is something the state believes the citizen will do.

By contrast, the 'Digital Masterplan 2025' serving the ASEAN nations is not an AI statute but a flexible framework for countries at different stages of digital development. Singapore's 'Smart Nation Initiative' ensures that while American companies provide the raw computing power and storage, the encryption keys and core citizen data are insulated from extraterritorial access. A Brookings Institution report recognises Singapore as the regional hub for AI standards. It points to Indonesia with its large population as having the scale and a formal national strategy to build capacity. It says Myanmar, by contrast, serves as a warning why rules must arrive before the cameras do.

The new Lords of the Rings

Tolkien's 'Lord of the Rings' fantasy is enjoying an unlikely revival in the AI and defence industries. Palantir, which takes its name from Tolkien's magical seeing-stone that can communicate across vast distances, integrates data from satellites, drones, logistics databases and battlefield systems, then turns them into military intelligence. In Britain the company is reported to be helping the government choose which weapons to buy. Anduril, another AI company, takes its name from Tolkien's mythical sword, the 'flame of the West', and builds autonomous AI systems that can sense and strike.



Technology firms such as Palantir and Anduril have become influential suppliers of AI-driven military and intelligence systems, borrowing their names from Tolkien's fantasy world.

The US military is accelerating adoption of AI. The Pentagon's 'Artificial Intelligence Strategy' made the priority explicit: 'The risks of not moving fast enough outweigh the risks of imperfect alignment'. Palantir's Maven system is becoming part of the core of America's and NATO's command-and-control architecture. Palantir is also one of Ukraine's key AI partners in the war with Russia, supporting intelligence analysis, strike planning, de-mining and air-defence strategy. The company's CEO, Alex Karp, claims he is on the Kremlin's hit list over his support for President Zelensky.

The Pentagon's standoff with another of its key suppliers, Anthropic, is raising concerns about the need for guardrails on military use of AI software. Anthropic insists on contractual safeguards against the use of its AI model Claude for domestic surveillance of Americans and for operating autonomous weapons without humans in the loop. The dispute remains unresolved.

The courts may need to decide whether democracies can allow private companies to restrict the use of their products on moral grounds. Should private companies, rather than elected governments, decide where the state must stop? The same technology can appear heroic on a battlefield and troubling in a hospital, police force or immigration system.

The Palantir dilemma

Software that helps Ukraine identify targets, track drones, and plan strikes provokes suspicion when repurposed for hospital management or domestic policing. Palantir's problem is not simply what its software does but the legacy of fear and suspicion it carries. According to its CEO, Palantir exists to 'disrupt' and make partner institutions 'the very best in the world' and, when necessary, 'to scare enemies and, on occasion, kill them'.

Published reports in the United Kingdom claim that Palantir is deeply embedded in the state apparatus having secured over 34 contracts across government departments totalling at least £670 million. These include a strategic partnership with the Ministry of Defence, and a highly controversial £330 million contract to run the National Health Service's Federated Data Platform. Concerns in Germany relate to the possibility of data held by US-headquartered companies being subject to US legal demands even when stored abroad. Swiss defence officials have also reportedly concluded that using Palantir software could risk national sovereignty, leading to rejection of the platform.



AI is increasingly being used to process battlefield intelligence, coordinate military operations and support decision-making in modern warfare.

Europe's Palantir problem is no longer just about privacy. It is about who ultimately controls the data, the software and the intelligence extracted from it. In Japan, Palantir has not produced the same public storm seen in Britain or Germany. But its partnerships with SOMPO and Fujitsu place it close to sensitive health, insurance, infrastructure and government data. South Korea, which has one of the highest densities of cameras and digital tracking systems in the democratic world, offers a concrete example of the risks and massive legal pushback that can challenge the use of biometric information for border control.

State voyeurism is not unique to China, the world's most powerful one-party state. A report by the Carnegie Endowment for International Peace shows that 51 percent of advanced democracies deploy AI surveillance systems. Democracies without checks and balances are especially vulnerable, because AI rewards centralisation. The world's wealthiest democracy, the United States, with its Palantir-linked systems for immigration and customs enforcement; the world's largest democracy, India, with its twelve-digit Aadhaar biometric identity programme; and the UK and Europe, with their battles over data governance, ethics, and sovereignty, all face challenges of accountability and civic transparency.

The state that knows too little cannot serve its citizens. The state that knows too much may cease to need their consent.

Sham Banerji is a veteran of the high-tech industry, having spent over three decades with Texas Instruments and Philips in the UK, the US, and India.

All images are AI generated