DEMOCRACY AND SOCIETY 21.08.2026 | Georgiana Banita

The terabyte trap

Swapping Palantir for a European equivalent may change who controls the technology, but not its democratic consequences

'We used to deal with diaries; today we deal with terabytes,' Germany's interior minister, Alexander Dobrindt, recently remarked as parliament considered legislation extending the federal police's digital surveillance and analytical powers. In Dobrindt's almost poetic formulation, the shift sounds mainly quantitative. Where villains once left behind physical notes and fingerprints, today, like everyone else, they shed innumerable digital traces across the surface of everyday life. No one is seriously proposing that modern police forces should conduct investigations with quills and filing cabinets. But access to vastly larger digital datasets does not produce more or better evidence by default, and it certainly won't abolish uncertainty. It merely relocates suspicion from the individual case to the population at large, and from private life into the civic sphere.

The difference between diaries and terabytes isn't, after all, merely a matter of upgraded storage capacity. A diary is a bounded record created for a purpose. Should its owner be suspected of a crime, it may become evidence subject to defined legal thresholds. And unless it happens to be the Goncourt brothers' sprawling chronicle of nineteenth-century Parisian life, its evidentiary reach remains tied to a single person. A terabyte of digital information is something else altogether. The systems that assemble it can hoover up an entire social world – every footstep, ping, photo, every murmur. It is not a bulkier diary in the sense implied by Dobrindt's analogy, but a mass of fragments, many of them produced inadvertently, gathered in advance of any demonstrated relevance. Dobrindt's rationale for data-driven policing therefore tacitly trades targeted evidence for unfiltered, ambient signal aggregation, which in a hyper-connected world can never run dry because to exist is to emit a detectable signal.

History repeating itself

This is where Europe's Palantir debate has wandered into a curious cul-de-sac. Critics reasonably object to dependence on a secretive American company whose politics and roots in the US security establishment have made it a democratic liability, prompting enthusiasm in Berlin and elsewhere for European alternatives to American-owned black boxes. Amid fears of cyberattacks, foreign jurisdiction, and reliance on vendors whose governments may no longer be dependable partners, wanting the servers closer to home is hardly irrational. Yet a German or French Palantir risks fostering the reassuring illusion that locally sourced surveillance is inherently superior to an imported global brand. The more consequential question is not whether Europeans' data is harvested by Silicon Valley or somewhere closer to Brussels, but why so much of public life is being colonised by AI policing in the first place.

In *The Structural Transformation of the Public Sphere*, Jürgen Habermas imagined a communicative space mediating between society and the state, an arena in which citizens make themselves publicly visible to one another and to authorities in order to exchange opinions, organise and – crucially – hold power to account. Historically, this took place in coffee houses, salons, associations, and newspapers; today, it also encompasses universities, broadcasters and, for better or worse, much of our online lives. Habermas' public sphere was, of course, always more aspirational than descriptive. Women, minorities, migrants, indeed anyone categorised as a problem rather than a participant, were routinely excluded from its protections. Yet its democratic principle remains difficult to dismiss: public life exists so that citizens can scrutinise power, not the other way around.

It would be naïve to focus on what these systems can detect at the expense of what they may also discourage.

This is precisely the distinction that technologies like Palantir (or European alternatives such as ChapsVision and DataWalk) risk eroding. Attending a demonstration, joining a campaign, donating to a cause – the sorts of activities we might call citizenship in action – can become data points to be connected and retrospectively reinterpreted through automated suspicion. The democratic bargain is thereby reversed. The public square ceases to be a medium of democratic accountability and turns instead into a source of machine-readable behavioural intelligence for the state. It would be naïve to focus on what these systems can detect at the

expense of what they may also discourage. How long before the possibility of exposure begins to inhibit participation and debate in civil society? And, the more cautious citizens become in expressing disagreement with power, the faster the mediating zone between society and the state contracts – until dissent retreats into the private sphere.

After living in Germany for 25 years, I had assumed that this atmosphere of self-censorship – reminiscent of Romania in the 1980s – was a thing of the past. Back then, much political criticism was forced into diaries, many of which were published after 1989. As governments move away from paper files and toward permanent digital records, citizens may again retreat into private spaces simply because the public sphere has become too legible to the state. The irony of Dobrindt's antithesis is that the terabyte may drive political criticism back into the drawer, the private room, or silence.

Democratic policing should secure the conditions of public participation, not convert participation itself into grounds for suspicion or into a stage for performing technological resolve.

None of this means that arenas of public discussion can dispense with police protection. The Habermasian public sphere is materially vulnerable, and data analysis can clearly serve legitimate and tightly bounded investigations. After the 2024 attack on Munich's Israeli Consulate, during which shots also struck the neighbouring NS Documentation Centre, Bavaria's VeRA system was used to cross-check investigative data against police records and search for extremist networks surrounding the attacker. Berlin's Christopher Street Day, meanwhile, is a textbook instance of embodied civic participation. Citizens appear before one another and before authorities to assert their rights and channel individual experiences of vulnerability and exclusion into collective political claims. Yet protecting such spaces is not the same as treating everyone who enters them – often precisely in order to form a counter-public to a society that marginalises or excludes them – as though they harboured nefarious intentions. Democratic policing should secure the conditions of public participation, not convert participation itself into grounds for suspicion or into a stage for

performing technological resolve.

The political pressure generated by the CSD attack is unlikely to remain confined to measures that might plausibly have prevented it. When parliament returns after the summer recess, the Bundestag must repeat its final vote on the Federal Police Bill before it can proceed to the Bundesrat. The attack is likely to provide the Interior Ministry with additional justification for its proposed facial-recognition and automated video-analysis powers, even though the problem in Berlin was not a failure to identify risk. Reporting by *NDR*, *WDR*, and the *Süddeutsche Zeitung* revealed that the perpetrator was already known to the authorities, classified as an Islamist *Gefährder*, and assessed as high risk by the Federal Criminal Police Office's RADAR-iTE tool. What the state lacked was not another apparatus for seeing and monitoring, but a clear threshold for intervention based on what it already saw. Here was the person the state itself had designated a *Gefährder* – what do we do? Perhaps he should have kept a diary. Terabytes, apparently, were not enough.

The answer to Palantir should therefore not be technological sovereignty alone, but constitutional restraint. German and European lawmakers must limit what data can be combined, prohibit open-ended analysis untethered to a specific and reviewable investigative purpose, mandate independent audits, and give citizens meaningful ways to challenge algorithmically generated suspicions, both legally and publicly. Systems must be designed around democratic boundaries, not laws rewritten to accommodate whatever systems are newly able to do. Europe should indeed reduce its dependence on Palantir. But a democratic society should also be careful not to confuse nationalising the machine with controlling the future it creates.



Georgiana Banita
Bamberg

Georgiana Banita is a qualified cultural scientist specialising in the United States. She heads the research project 'Safety for all: Police culture in an immigrant society' at the University of Bamberg.