The Talking Rights blog article, 4.9.2025
https://talkingrights.org/2025/09/04/palantir-human-rights/
Talking Rights is based at the Institute for Human Rights
at Åbo Akademi University.

The Case of Palantir: The underappreciated multifaceted human rights threat(s) of subcontracting national defence

In recent decades, democratic states have developed a tendency to place themselves into existential dependence on private companies. As such, in many policy fields, private actors such as asset-management-cooperations or Big-Tech-Companies act with power that in some ways rivals that of nation-states.

In the national security arena, the potential risks connected to dependence on such private interests were prominently displayed recently, when Elon Musk, in the course of his dispute with U.S. President Donald Trump, threatened to decommission SpaceX's "*Dragon*" spacecraft, which would have left the United States temporarily without the means to reach the International Space Station. This episode forms part of a series of comparable pressures exerted by Musk on the governments of Poland and Ukraine, with the implied threat of excluding the Ukrainian army from use of the Starlink satellite network.

The possibility of democracies being forced to direct their policy decisions at the mercy of a few non-democratically legitimised billionaires owning services necessary for national security, without available alternatives also exists in multiple Western countries through the uptake of services from the controversial U.S. corporation Palantir. Palantir's software not only poses multiple direct human rights concerns in its application, but also more importantly, though less acknowledged, puts into question the future ability of states to effectively discharge their obligations to protect from human rights violations occasioned by private actors in fulfillment of the right to remedy under Art. 2 (3) ICCPR and the right to equality before courts and tribunals under Art. 14 ICCPR.

About Palantir

Palantir was founded in 2004 by several entrepreneurs from the PayPal milieu and, building on PayPal's fraud-detection software, quickly became the world's leading—and currently seemingly unreplaceable— anti-terror data analysis firm through early field trials in Afghanistan and Iraq. Palantir's software has been and is still being used across various institutions in multiple

democratic states such as e.g. the U.S., the U.K., NATO, Israel, Ukraine, France, Denmark, and multiple federal states within Germany, with plans for nationwide usage.

From a human-rights standpoint, this utilisation is problematic in many respects.

Direct Problems concerning the software application

Criticism to date has focused primarily on Palantir's disregard for its responsibility (according to the (formally non-binding) UN Guiding Principles on Business and Human Rights) to respect human rights in the realm of software applications. Among its most well-known alleged human rights violations are infringements to the non-discrimination principle according to Art. 2 ICCPR through disproportionate criminalization of ethnic minorities (the company was also sued by the U.S. government in 2016 for racist hiring practices, which was settled out of court later on), the technical support for frequent violations of the Right to Privacy in Art. 17 ICCPR by the U.S. Immigration and Customs Enforcement, and its temporary cooperation with the security firm HB Gary Federal to develop proposals for attacking WikiLeaks' infrastructure and blackmailing its supporters, contrary to the protection of freedom of expression and press according to Art. 19 ICCPR.

Indirect Problems

There is also a danger that states, the primary implementers of the ICCPR, could become systematically dependent on Palantir, making effective implementation measures against the company and its allies practically impossible. As the examples above illustrate, comparable dependencies already exist—e.g., Ukraine's dependence on Musk and Starlink—which render any effective legal action or even criticism a national security risk and have, in the war against Russia, prevented certain operations because Musk did not endorse them. When individualised private interests exert such control over state functions, the enforcement of wider public interest by legitimate state forces becomes endangered. In relation to Palantir, dependency risk arises because—just as in the Starlink case—no alternatives of remotely comparable quality exist.

Palantir and its political backers counter that customers are supposedly safe from external influence once they purchase the product, because the software operates on platforms in independent data centres and in some cases, the authorities were granted the possibility to review the original source code. Yet Palantir itself acknowledges that its software products require continual updates and upgrades in our ever-changing world to maintain functionality. This presents two risks: Palantir may introduce backdoors in updates that were absent in the original version, and it could withhold future updates, significantly degrading the platform's performance and associated security services.

In theory states may have some leverage over Palantir by refusing payment or possibly even seeking reimbursement over human rights abuses through procurement or contract law (though in most cases the contracts are not publicly accessible, and therefore it is unknown whether they include human rights clauses), the problem remains the same in that it is, practically-speaking, difficult to enforce any law against a company upon which the legislating state is reliant for maintaining national security. Furthermore, when push comes to shove, any purely financial threat is unlikely to hold decisive sway over either Karp or Thiel, since either of them is estimated to be among the 200 richest people in the world with an estimated net worth far surpassing 10 billion $ and given that they seem in many ways more ideologically than purely financially motivated.

Ultimately, it is a question of trust: Public security authorities must decide whether to trust Palantir's leadership, which seems a doubtful enterprise considering that the responsibility largely lies with the founders, one of which is also its acting CEO.

Libertarian tech billionaire Peter Thiel has on multiple occasions publicly uttered opinions that cast doubt on his allegiance towards human rights: He has described women's suffrage as turning "*capitalist democracy into an oxymoron*". After spending many of his formative years in Namibia and South Africa under Apartheid rule (which he allegedly defended later on) he went on to write "*The Diversity Myth*" (a defense of "*western civilization*" against "*multiculturalism*") in 1995 shortly after Nelson Mandela became President for the first time. His argumentation generally endorsed (though usually in carefully chosen words) a worldview that bears striking resemblances with the rationalizations of South African white nationalist narratives. Recently, it seems to be doubtful whether he wishes humanity to survive as a species at all or whether this is irreconcilable with his longstanding fascination with transhumanism in order to avoid death.

Karp has not publicly made comparably extreme statements and (controversially) even considers himself to be a progressive, but has shifted toward more conservative sentiment. In recent years, he has supported ethically questionable decisions, such as drastically under-staffing Palantir's civil rights division and continuing to support the Trump administration's harsh deportation programs against the wishes of hundreds of Palantir employees.

Outlook

As things stand, there can be little doubt that Palantir's rise currently seems bound to continue. Since President Trump's inauguration, the company has won more than $900 million in federal contracts, laying the financial and training data possession ground for enabling an increase of its technological lead against potential competitors. The clique associated with Palantir has also (though technically separated from the company itself), primarily under the responsibility of Palantir CTO Shyam Sankar and early Palantir employee Ryan Podolsky, started a coordinated effort to expand its collective influence beyond the realm of national security by pitching the new firm "*Founders Films*", a production company that, within the ongoing, notably right-wing shift in contemporary U.S. media, is designed to propagate American exceptionalism, "*name America's enemies", and generally push for* confrontation with the nuclear power China. In other words, after creating the supply of military technology, Palantir executives seem now determined to create the largest possible demand for it. From a conventional perspective, it might seem unlikely that national security experts would be able to build a commercially successful movie company but given Palantir's AI expertise and the sharply growing role of AI in media production, conventional views might become outdated quite rapidly. This could result in a situation in which not only the conventional three branches of government will depend on Palantir, but its executives are also going to have a significant sway over the media, often characterised as the fourth branch of government.

While the direct human rights problems connected to transnational companies have to some degree been recognised by states, and some efforts have been undertaken or are in planning stages to address them, changing specific legal provisions cannot solve the dependency problem, meaning that, as long as such an existential dependency exists and states cannot convincingly fulfill their aspiration to hold the monopoly on the legal (potential) use of force against anyone, human rights

are in danger.

Conclusion

In summary, there are grave human rights concerns about deploying Palantir, even though there is undeniably a need for public security defence by software means. Therefore, states are imperatively called upon to develop state-owned alternatives that can provide the same capacities over which Palantir currently enjoys a quasi-monopoly. While inherently avoiding the corporate reliance risk, the other human rights issues discussed above (concerning infringements of the non-discrimination principle according to Art. 2 ICCPR, violations of the Right to Privacy in Art. 17 ICCPR, etc.) could naturally also arise within the framework of a state-developed software. Therefore, it is imperative that, while absolute transparency is of course not possible in the realm of natural security, strict accountability mechanism must oversee the development as well as the application of the public alternative. This could, for example, happen by virtue of a distinct parliamentary oversight committee dedicated to this specific task, which would at the same time be able to provide the warranted level of confidentiality while also constituting a democratically legitimised form of accountability institution, comparable, e.g. to the Intelligence and Security Committee of Parliament (ISC) in the U.K.

All this is to assure that, regardless of one's exact ideological stance on specific issues, the smallest common denominator among defenders of human rights and democracy should be to keep their open enemies away from state security matters, to keep the possibility of holding them accountable alive. At least publicly, Palantir has recently even vaguely supported that notion, stating that "*Palantir believes that we — as contractors to the federal government — should not be in a position to set policy on behalf of the US Government*". Now it is upon government officials to hold them to their word by ending/ preventing the reliance on the firm's services so that policy can indeed be set, no matter what Palantir's owners have in mind.