Disclaimer: This two-pager has been prepared by the CKN Secretariat and should not be considered the work of the individuals listed as authors of the report.

#36 Evaluating Data Security in Chinese Drones and Smart Vehicles

Authors: Rogier Creemers, John Lee

April 2025

Key Takeaways

- China increasingly treats data as both a strategic economic resource and a national security issue through an evolving system of data governance laws and regulations.
- The PIPL creates limited risks for European users abroad, while the Data Security Law remains more ambiguous regarding possible government access to data.
- Chinese smart vehicles and drones generally comply with international and EU cybersecurity standards and incorporate many privacy-protecting features.
- Independent audits of Chinese EVs and drones have identified ordinary engineering and cybersecurity vulnerabilities rather than evidence of systematic espionage backdoors.
- The report concludes that current evidence does not justify blanket restrictions on Chinese smart vehicles or drones purely on the basis of nationality.

Recommendations

- European governments should continue strengthening and updating technology-neutral cybersecurity and data governance standards for connected vehicles and drones.
- Regulators should focus on product-specific technical risks demonstrated through audits and testing rather than relying primarily on political assumptions about vendor nationality.
- Authorities should expand independent auditing, penetration testing and regulatory oversight capacity for smart vehicles, drones and related cloud services.
- EU institutions should clarify how existing legislation such as the GDPR and Data Act applies to connected vehicles, drones and associated data flows.
- Regulators should apply additional safeguards for sensitive government, military and critical infrastructure environments, including tailored restrictions for specific high-risk use cases.

Executive Summary

This report evaluates whether China's legal and regulatory frameworks for data governance create security risks for Dutch and European governments, companies and citizens through the use of Chinese smart connected vehicles (ICVs) and drones. It examines both the broader Chinese data governance environment and the technical and regulatory characteristics of Chinese-made EVs and UAVs.

The report finds that China has increasingly treated data as both a strategic economic resource and a national security issue. Over the past decade, China has developed an extensive legal framework for data governance, centred on the Personal Information Protection Law (PIPL), the Data Security Law (DSL), cybersecurity legislation and sector-specific regulation for smart vehicles and drones. Chinese authorities have simultaneously promoted the development of data-driven technologies while strengthening security and control mechanisms around sensitive data flows.

At the same time, growing geopolitical concerns have led Western governments to scrutinise Chinese smart vehicles and drones over fears of espionage, surveillance and cyber vulnerabilities. Much of this debate focuses on the possibility that Chinese firms could be compelled to cooperate with Chinese intelligence services under the National Intelligence Law. However, the report concludes that the legal picture is more complex than often assumed. The PIPL primarily applies to personal information processing within China and therefore creates very limited risks for European users of Chinese vehicles or drones abroad. The DSL is more ambiguous, particularly regarding access to data for national security purposes, but many aspects of its implementation remain underdeveloped.

The report's technical case studies on Chinese EV manufacturers such as BYD and Nio, and drone manufacturer DJI, find no clear evidence of systematic espionage capabilities or major cybersecurity backdoors. Chinese smart vehicles and drones generally comply with international and EU cybersecurity standards, including UN Regulations 155/156/157 for vehicles. Many core cloud, computing and software services used in these products are supplied by US and European firms such as Amazon Web Services, Nvidia and Microsoft. Independent European and US audits of Chinese drones and connected vehicles have generally identified ordinary engineering and privacy-management vulnerabilities rather than malicious design features.

Nevertheless, risks cannot be entirely excluded. The report notes that Chinese intelligence services face relatively few independent legal constraints and that political pressure could in principle be exerted on Chinese firms. Vulnerability disclosure requirements under Chinese cybersecurity regulations may also create opportunities for Chinese authorities to obtain information on exploitable software weaknesses. However, the report argues that any systematic misuse of Chinese smart vehicles or drones for espionage would likely be rapidly detected and would carry major economic and political costs for China's globally competitive technology firms.

Overall, the report concludes that the currently available evidence does not justify blanket bans or separate regulatory frameworks targeting Chinese smart vehicles and drones solely on the basis of their nationality. Instead, it recommends maintaining strong, technology-neutral cybersecurity and compliance standards, improving auditing and testing capacity, clarifying EU legislation, and applying additional scrutiny only where product-specific risks can be demonstrated.