

**Question for written answer E-000056/2026  
to the Commission**

Rule 144

**Nicolás González Casares (S&D), Laura Ballarín Cereza (S&D)**

**Subject:** Data privacy and security risks posed by AI and browser extensions harvesting AI chat conversations

A recent cybersecurity investigation found that several widely used browser extensions that were advertised as privacy or security tools were secretly collecting users' AI chat conversations. According to Koi Security, this data collection could not be disabled without uninstalling the extension, it affected over 8 million users, and it involved transmitting complete AI prompts and responses, timestamps and session data to third-party servers for marketing analytics – despite the extensions being promoted with trust badges that may have misled users.

In the light of the above,

1. Does the Commission consider that the automatic collection and commercial sharing of users' private AI interactions – often involving highly sensitive personal, health, financial or proprietary information – without clear, informed and granular consent, constitutes a breach of EU data protection and AI governance frameworks?
2. What measures will the Commission take to ensure digital marketplaces effectively enforce platform policies and prevent the use of browser extensions that engage in covert data harvesting from being promoted with trust signals (e.g., 'featured' badges) that imply user safety?
3. In relation to AI governance and cybersecurity, does the Commission plan to propose specific regulatory guidance, additional safeguards or enforcement action to address the privacy risks associated with AI services and with browser extensions that intercept AI service communications?

Submitted: 9.1.2026