

**Question for written answer E-003882/2026
to the Commission**
Rule 144
Jorge Buxadé Villalba (Pfe)

Subject: Cyber-attack against Renfe and Adif: protecting travellers and ensuring accountability

On 25 September news broke of a cyberattack on Renfe and Adif, which report to Óscar Puente's Ministry of Transport. Renfe claimed that only limited information was accessed and denied having any evidence of any national ID numbers being stolen. However, on 27 September the newspaper El Mundo reported¹ – citing sources close to the investigation – that more than 150 million data points had been stolen, including national ID numbers, addresses and personalised ticket records.

The gravity of these revelations demands an investigation into possible security failings and whether Renfe withheld information from those affected. Meanwhile, the Sánchez government is lagging behind in transposing the SRI 2 Directive, causing the Commission to open proceedings against them at the CJEU².

1. What action will the Commission take vis-à-vis the Spanish authorities to clarify any potential shortcomings in prevention and supervision, as well as the liabilities arising from this cyberattack and breach of EU law?
2. Will it request information on compliance with the GDPR, in particular as to what Renfe was aware of when it issued its statement and whether it provided those affected with accurate information in a timely manner?
3. What measures will it take to address the delay in transposing SRI 2 with a view to enforcing it and verifying that Spain ensures effective oversight of railway cybersecurity?

Submitted: 28.9.2026

¹ <https://www.elmundo.es/economia/empresas/2026/09/27/6ab9544a21efa0fd208b4576.html>.

² <https://digital-strategy.ec.europa.eu/es/news/commission-refers-ireland-spain-france-and-netherlands-court-justice-failing-transpose-rules>.