



PRESS RELEASE No 42/26

Luxembourg, 19 March 2026

Advocate General's Opinion in Case C-354/24 | Elisa Eesti

Advocate General Ćapeta: Member States may exclude hardware and software from 2G-4G and 5G telecommunications infrastructure on the basis that the manufacturer of that equipment poses a risk to national security

However, measures taken to protect the national security of a Member State must still be proportionate under EU law

In 2022, Elisa Eesti AS, an Estonian telecommunications provider, applied for authorisation from the Estonian authorities to use hardware and software from the Chinese telecommunications equipment manufacturer Huawei for use in its 2G-4G and 5G telecommunications networks. The competent Estonian authorities considered that hardware and software to pose a risk to Estonia's national security on the basis of the 'high-risk' nature of Huawei. That decision has been challenged before the Administrative Court, Tallinn, which requested a preliminary ruling.

In her Opinion, **Advocate General Tamara Ćapeta proposes that the Court find that the Member States may, in principle, exclude hardware and software from their telecommunications infrastructure on the basis that the manufacturer of that equipment poses a risk to their national security.**

However, the Advocate General also highlights that any decision taken on the basis of national security grounds must be **subject to judicial review**, including as regards **their proportionality. While a risk assessment may be different for third country equipment manufacturers than for EU manufacturers of the same equipment, such a decision cannot be based on a general suspicion.** Instead, it must involve a specific assessment of the use of the intended equipment and the risks associated therewith.

In the circumstances of the particular case, the Advocate General also highlights that the relevant rules of EU law, the European Electronic Communications Code,¹ specifically provide for certain security requirements for national telecommunications networks and services. By virtue of those EU law requirements, **EU and national security interests converge.** In such a situation, the competent national authorities may draw on risk assessments undertaken by the EU institutions and other national and EU bodies.²

Finally, the Advocate General observes that a restriction on the use of hardware and software by virtue of the risk of that equipment to EU and Member State security **does not constitute a deprivation of property but rather a limitation on the use of that property, within the meaning of Article 17(1) of the Charter.** In such a case, a company is, in principle, **not entitled to compensation unless** the national court finds that **the burden** arising from that type of restriction **is disproportionately heavy, even if necessary.**

NOTE: The Advocate General's Opinion is not binding on the Court of Justice. It is the role of the Advocates General to propose to the Court, in complete independence, a legal solution to the cases for which they are responsible. The Judges

of the Court are now beginning their deliberations in this case. Judgment will be given at a later date.

NOTE: A reference for a preliminary ruling allows the courts and tribunals of the Member States, in disputes which have been brought before them, to refer questions to the Court of Justice about the interpretation of EU law or the validity of an EU act. The Court of Justice does not decide the dispute itself. It is for the national court or tribunal to dispose of the case in accordance with the Court's decision. That decision is similarly binding on other national courts or tribunals before which a similar issue is raised.

Unofficial document for media use, not binding on the Court of Justice.

The [full text](#) of the Opinion is published on the CURIA website on the day of delivery.

Press contact: Jacques René Zammit ☎ (+352) 4303 3355.

Pictures of the delivery of the Opinion are available from '[Europe by Satellite](#)' ☎ (+32) 2 2964106.

Stay Connected!



¹ [Directive \(EU\) 2018/1972](#) of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

² See, in particular, Communication from the Commission, Implementation of the 5G cybersecurity Toolbox, COM (2023) 4049 final.