



Phone: +44 800 999 3237 | +1 800 356 6547 | +852 2965 1424 | www.mlex.com
customerservices@mlex.com

Huawei, telecom operators may see EU legal clarity on national security bans

By **Matthew Newman**

October 6, 2026, 12:53 GMT | Comment

Huawei Technologies and other telecom equipment providers could get clearer legal guidance in the coming months on the limits of national security restrictions, as courts consider two legal challenges to those measures and EU legislators debate new rules for critical technology supply chains. A ruling by the EU Court of Justice may set a baseline for national regulators and EU legislators on how to handle exclusion orders that are based on national security questions.

Huawei Technologies and other telecom equipment providers could get clearer legal guidance in the coming months on the limits of national security restrictions, as courts consider two legal challenges to those measures and EU legislators debate new rules for critical technology supply chains.

The disputes concern restrictions imposed by Sweden in 2020 and Estonia in 2022 on the use of China-based Huawei equipment in mobile networks, including those used to provide high-speed 5G services.

In a case before the EU Court of Justice, judges are considering national security restrictions on Estonian operator Elisa Eesti* and the application of EU telecom law and property rights apply to these restrictions. The Swedish arbitration concerns Huawei's rights as an investor under an international treaty.

The EU court's interpretation would bind national courts across the bloc addressing similar EU-law issues. The investment tribunal would separately assess Huawei's treaty claims.

In parallel, EU lawmakers and governments are discussing a framework to identify non-EU countries that pose cybersecurity risks to critical technology supply chains under a proposed revision of the Cybersecurity Act, known as CSA2 (see here).

The timing of the courts' decisions, and how they may influence the EU legislative talks, is under scrutiny. A ruling by the EU Court of Justice may set a baseline for national regulators and EU legislators on how to handle exclusion orders that are based on national security questions.

These cases are closely watched because telecom operators face substantial equipment replacement costs. A July study by GSMA Intelligence, commissioned and sponsored by seven European operator groups, estimates that removing high-risk vendors' equipment from EU mobile, fixed and transport networks under the CSA2 framework could cost as much as €40 billion.

— EU debate —

Equipment providers' exposure to EU cybersecurity restrictions remains under debate. Governments and lawmakers are considering who should designate high-risk suppliers, and whether the process should target countries or individual companies.

The European Commission's original proposal would allow it to designate non-EU countries posing cybersecurity risks through implementing acts adopted with oversight from member-state

representatives. These are non-legislative measures designed to ensure EU law is applied uniformly across member states.

A Sept. 22 draft from the Council of the EU, which represents national governments, would instead have the commission submit a designation proposal to the council.

Markéta Gregorová, the lawmaker leading the European Parliament's review, has proposed removing country designations and having the commission assess and list individual high-risk suppliers instead.

— EU court case —

Elisa Eesti applied in 2022 for authorization to use Huawei hardware and software in its 2G-4G and its 5G networks. Estonian law requires operators to obtain authorization to use network hardware and software.

Estonian authorities considered the equipment a national security risk because they regarded Huawei as a high-risk supplier. They granted permission to use it until Dec. 31, 2025, for 5G services and Dec. 31, 2029, for 2G-4G services. Elisa challenged those decisions.

The Administrative Court in Tallinn referred questions to the EU Court of Justice about the application of EU law, and whether the restrictions amounted to a deprivation of property requiring compensation.

On March 19, Advocate General Tamara Ćapeta said in a nonbinding opinion, which the court is under no obligation to follow, that the authorization regime falls within EU law. She said EU countries may, in principle, exclude hardware and software from their networks when the manufacturer poses a national security risk.

But such decisions must be subject to judicial review, including scrutiny of their proportionality. Risk assessments may differ for non-EU manufacturers, but decisions cannot rest on "a general suspicion." They must assess the intended use of the equipment and the associated risks.

Under the EU Charter of Fundamental Rights, the restrictions limit the use of property rather than deprive the operator of it, Ćapeta said. A company is therefore, in principle, not entitled to compensation unless the national court finds that even a necessary restriction imposes a disproportionately heavy burden.

— Arbitration case —

Huawei's arbitration followed a Swedish authority's decision in October 2020 to impose spectrum-auction conditions excluding Huawei and Chinese supplier ZTE products from new network installations on national security grounds. The conditions also required their existing products to be removed by Jan. 1, 2025.

Huawei's Swedish subsidiary challenged the decision in administrative courts. Huawei submitted its international arbitration request on Jan. 7, 2022, while the domestic appeal was pending.

Huawei called the regulator's decision "blatantly discriminatory," and said it deprived the company of "the benefits of its long-term investments in the country."

It also alleged that the measures lacked transparency and breached Sweden's treaty obligations, including fair and equitable treatment and protection against uncompensated expropriation.

— Wider restrictions —

Huawei and ZTE face restrictions elsewhere in Europe.

Germany agreed with mobile operators in July 2024 that they would stop using critical Huawei and ZTE components in 5G core networks by the end of 2026. Operators must also replace critical functions of the suppliers' network management systems in 5G access and transport networks by the end of 2029.

In France, operators need national security authorization for certain 5G equipment. Free Mobile challenged refusals to authorize Huawei equipment at thousands of sites.

In March 2025, the State Council, France's highest administrative court, overturned a ruling by the Paris Administrative Court of Appeal and sent the case back to that court for reconsideration. It said protecting national security didn't exempt authorities from considering freedom of trade and competition rules.

An EU court decision would give a strong signal to EU government authorities, which may rule on cases on national security grounds.

For European operators that have relied heavily on Chinese suppliers, these rulings could serve as a critical benchmark for the entire European telecom industry and could provide essential legal clarity.

**The case number is C-354/24 — Elisa Eesti.*

Please email editors@mlex.com to contact the editorial staff regarding this story, or to submit the names of lawyers and advisers.

Tags

Sections: Data Privacy & Security, Technology

Industries: Media & Telecommunications

Geographies: Europe, European Union Member States

Topics: Cybersecurity, Future Mobility

Related Case File(s)

[Data Privacy & Security - Cybersecurity legislation \(EU\)](#)