

СЪД НА ЕВРОПЕЙСКИЯ СЪЮЗ
TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA
SOUDNÍ DVŮR EVROPSKÉ UNIE
DEN EUROPÆISKE UNIONS DOMSTOL
GERICHTSHOF DER EUROPÄISCHEN UNION
EUROOPA LIIDU KOHUS
ΔΙΚΑΣΤΗΡΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ
COURT OF JUSTICE OF THE EUROPEAN UNION
COUR DE JUSTICE DE L'UNION EUROPÉENNE
CÚIRT BHREITHIÚNAIS AN AONTAIS EORPAIGH
SUD EUROPSKE UNĚJE
CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA



EIROPAS SAVIENĪBAS TIESA
EUROPOS SĄJUNGOS TEISINGUMO TEISMAS
AZ EURÓPAI UNIÓ BÍRÓSÁGA
IL-QORTI TAL-ĠUSTIZZJA TAL-UNJONI EWROPEA
HOF VAN JUSTITIE VAN DE EUROPESE UNIE
TRYBUNAŁ SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ
TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA
CURTEA DE JUSTIȚIE A UNIUNII EUROPENE
SÚDNY DVOR EURÓPSKEJ ÚNIE
SODIŠČE EVROPSKE UNIJE
EUROOPAN UNIONIN TUOMIOISTUIN
EUROPEISKA UNIONENS DOMSTOL

OPINION OF ADVOCATE GENERAL
ĆAPETA
delivered on 19 March 2026 ¹

Case C-354/24

Elisa Eesti AS

v

**Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu,
Tarbijakaitse ja Tehnilise Järelevalve Amet**

(Request for a preliminary ruling from the Tallinna Halduskohus (Administrative Court, Tallinn, Estonia))

(Preliminary ruling – Telecommunications services – Directive (EU) 2018/1972 – Article 40(1) and Article 41(1) – Security of networks and services – 5G functionality – Authorisation procedure – ‘High-risk’ suppliers of hardware and software – Prohibition of ‘high-risk’ hardware and software on grounds of national security – Article 4(2) TEU – Article 17(1) of the Charter – Proportionality – Intensity of review – Positive measures in case of third-State influence or control)

¹ Original language: English.

I. Introduction

1. How do measures taken by a Member State with a view of protecting its national security interact with EU legislation enacted to ensure the functioning of the internal market in electronic communications networks and services?

2. Most importantly, are such national measures excluded from the scope of application of Directive (EU) 2018/1972 (the European Electronic Communications Code, ‘the EECC’),² because they were taken for national security reasons, and do they therefore elude judicial review of their proportionality under EU law?

3. Those questions arise in the context of legislation adopted in Estonia to put in place an *ex ante* authorisation procedure for the use of hardware and software in the provision of electronic communications networks and services. That procedure enables the competent authorities to prohibit the use of certain equipment if deemed to pose a risk to national security.

4. The applicant in the main proceedings, Elisa Eesti AS (‘the applicant’), a subsidiary of the Finnish telecommunications company Elisa Oyj, is one of three providers of nationwide mobile telecommunications networks and services in Estonia. Before the Tallinna Halduskohus (Administrative Court, Tallinn, Estonia) (the referring court), it challenges a decision by which the competent Estonian authorities refused to grant it an authorisation for the use in its telecommunications network of certain 2G-4G and 5G hardware and software. That decision was, inter alia, adopted because that equipment was manufactured by a Chinese telecommunications company, Huawei Corporation (‘Huawei’), which the Estonian authorities considered to be a ‘high-risk’ supplier of such equipment.

II. The legal and factual context of the present case and the questions referred for a preliminary ruling

A. Background information on 5G telecommunications infrastructure and technology

5. Understanding the background to this case requires a minimum level of explanation of the infrastructure underlying 5G functionality. That is what I will start with.

6. A mobile telecommunications network is traditionally composed of two parts. The first and central part of that infrastructure is *the core network*. It contains the central equipment that controls the entire network and is designed as

² Directive of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ 2018 L 321, p. 36).

the main conduit to interconnect all traffic end points, aggregating and transferring network traffic at high speed.³ The second part of that infrastructure is *the mobile radio network*. The latter is composed of base stations which divide a larger service area into ‘cells’, and to which cellular devices, such as mobile phones, can connect across a Member State’s mobile network.⁴ This part of the mobile network is sometimes referred to as the ‘edge’ network.

7. Telecommunications technology is referred to by ‘generations’. 2G, 3G and 4G are successive generations of non-analogue mobile network technology. The fifth generation of that technology – 5G – is designed to replace the current 4G standard in the future.⁵ 5G technology is characterised by high speed and data capacities and lower latency (delay).

8. The European Commission considers 5G technology to be an important component of building high-speed and high-capacity networks in the European Union, for the benefit of the economy and society as a whole.⁶

9. As arises from the order for reference and the national file, 5G technology can be separated into ‘non-stand-alone’ 5G and ‘stand-alone’ 5G functionality. *Non-stand-alone* 5G is the technology that is built on top of the existing network

³ See, to that effect, Sendin, A., Sanchez-Fornie, M.A., Berganza, I., Simon, J., Irritoa, I., *Telecommunication Networks for the Smart Grid*, Artech House, Boston, 2016, p. 176. Due to its fundamental importance to the telecommunications infrastructure as a whole, the core network is sometimes referred to as the ‘backbone’ or ‘brain’ of a mobile network. See, generally on that point, the NATO Cooperative Cyber Defence Centre of Excellence, which has described the core network as ‘fundamental infrastructure and therefore ... an essential national interest, bearing national security implications.’ See NATO Cooperative Cyber Defence Centre of Excellence, Kaska, K., Beckvard, H. and Minárik, T., ‘Huawei, 5G and China as a Security Threat’, 2019, p. 15, available at: <https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf>.

⁴ See, for example in Germany, Federal Office for Information Security, ‘5G Risk Analysis, Framework Document: Methodology, Risk Scenarios and Results’, 2025, p. 21, which explains that ‘the Radio Access Network (RAN) contains 5G base stations ... with a radio interface ... that provides connectivity for mobile devices’ (available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/5G/5G_Framework_Document.pdf?__blob=publicationFile&v=4).

⁵ In certain Member States, 2G and 3G networks are already in the process of being switched off: see, for example, in the case of Ireland, Commission for Communications Regulation, ‘2G/3G Switch off: Guidance for Mobile Network Operators’, ComReg 24/61, 30 July 2024, available at: <https://www.comreg.ie/media/2024/07/ComReg-2461.pdf>.

⁶ The Commission expressed that position already in 2016, and later built upon it. See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, ‘5G for Europe: An Action Plan’, COM(2016) 588 final, p. 4, in which the Commission explains that ‘an ambitious 5G introduction timeline is essential for Europe to have a leading position and to take early advantage of the new market opportunities enabled by 5G, not only in the telecom sector, but in the whole economy and society.’

layer of 2G-4G infrastructure.⁷ Communication therefore still occurs to and from the ‘edge’ and ‘core’ communications network. *Stand-alone* 5G networks establish their own radio network and so do not depend on the ‘older’ 2G-4G infrastructure, or the core network. Stand-alone 5G devices therefore make up their own, independent network infrastructure without first passing through the core network. On that basis, they can directly communicate with one another without passing through the ‘core’ of the telecommunications infrastructure. Because of that characteristic, stand-alone 5G technology will be capable of connecting many more devices than ever before in the ‘internet of things’.⁸

10. It arises from the order for reference and the case file that the applicant’s core network is composed of hardware and software manufactured by the Swedish company Telefonaktiebolaget LM Ericsson (‘Ericsson’) and the Finnish company Nokia Corporation (‘Nokia’) and that its mobile radio network is composed of hardware and software manufactured by the Chinese company Huawei.

11. The present dispute only concerns the applicant’s mobile radio network, that is to say the edge network.

B. The legal and factual background to the main proceedings

12. On 23 March 2022,⁹ the applicant submitted to the Tarbijakaitse ja Tehnilise Järelevalve Amet (Office of Consumer Protection and Technical Supervision) (‘the TTJA’) an application for authorisation to use, in its edge network, (i) Huawei 2G-4G hardware and software already present therein and (ii)

⁷ In point 2(a) of Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ 2019 L 88, p. 42) (‘the Cybersecurity Recommendation’), the Commission defines ‘5G networks’ as ‘a set of all relevant network infrastructure elements for mobile and wireless communications technology used for connectivity and value-added services with advanced performance characteristics such as very high data rates and capacity, low latency communications, ultra-high reliability, or supporting a high number of connected devices. These may include legacy network elements based on previous generations of mobile and wireless communications technology such as 4G or 3G. 5G networks should be understood to include all relevant parts of the network.’

⁸ See, for example, the 2022 Special Report of the European Court of Auditors, in which it is stated that ‘by the end of 2018, there were an estimated 22 billion connected devices in use worldwide[, and that] this figure is forecast to increase to around 50 billion by 2030, creating a massive web of interconnected devices spanning everything from smartphones to kitchen appliances. The global consumption of data is expected to jump from 12 exabytes of mobile data traffic per month in 2017 to over 5 000 exabytes by 2030.’ See European Court of Auditors, *5G roll-out in the EU: delays in deployment of networks with security issues remaining unresolved*, Special Report 03/2022, Publications Office of the European Union, Luxembourg, 2022, p. 7, available at: https://www.eca.europa.eu/Lists/ECADocuments/SR22_03/SR_Security-5G-networks_EN.pdf.

⁹ I should observe that while the order for reference and the applicant’s observations stipulate 23 March 2022 as the date at which the applicant applied for authorisation, according to the Estonian Government’s observations and parts of the national file, including Decision No 1-7/22-436 of 25 November 2022 of the TTJA, that application is dated 18 March 2022.

Huawei 5G hardware and software to be introduced therein from 1 June 2022 (together, ‘the hardware and software at issue’).

13. That application was filed on the basis of the elektroonilise side seadus (Estonian Electronic Communications Act, ‘the ESS’).¹⁰ The referring court explains that the ESS inter alia transposes the EECC.

14. Chapter 8 of the ESS lays down certain requirements for the provision of electronic communications services in Estonia. Paragraph 87²(1) thereof requires that communications undertakings put in place appropriate technical and organisational measures to manage the risks relating to the security and integrity of a communications service and network. Paragraph 87³(1) of the ESS mandates that the hardware and software used in the provision of communications services in a communications network must not pose a risk to national security. Accordingly, as Paragraph 87³(6) thereof mandates, a communications undertaking is obliged to apply for an authorisation for the use of hardware or software in a communications network from the TTJA.

15. Pursuant to Paragraph 87³(2) of the ESS, a risk to national security is established on the basis of the high risk posed by the manufacturer or provider of maintenance or support services (point 1 thereof) or due to the risk arising from the technical characteristics or configuration of the hardware or software (point 2 thereof). The high-risk nature of a manufacturer or provider of maintenance or support services is assessed on the basis of 12 criteria, laid down in Paragraph 87³(3) of the ESS.¹¹

¹⁰ An English translation of that text may be found at <https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/528102025002/consolide>.

¹¹ Those 12 criteria are the following: ‘1) the producer or provider of maintenance or support services has its registered office or head office in a country ... which is not a [M]ember [S]tate of the European Union, the North Atlantic Treaty Organisation [(NATO)] or the Organisation for Economic Co-operation and Development [(OECD)]; 2) the principles of democratic rule of law are not observed or human rights are not respected in the country of domicile of the producer or provider of maintenance or support services; 3) the intellectual property, personal data or business secrets of persons of other countries are not protected in the country of domicile of the producer or provider of maintenance or support services; 4) the country of domicile of the producer or provider of maintenance or support services exhibits aggressive behaviour in cyberspace; 5) the [M]ember [S]tates of the European Union, NATO or OECD have attributed cyber-attacks to the country of domicile of the producer or provider of maintenance or support services; 6) the producer or provider of maintenance or support services is subjected to the government or state authority of the country of domicile or other foreign country that has no independent judicial control; 7) the country of domicile of the producer or provider of maintenance or support services or another foreign country may oblige it to act in a manner posing a risk to the national security of Estonia; 8) the economic activities of the producer or provider of maintenance or support services are not based on market-based competition or no adequate conditions have been created for this in the country of domicile; 9) the ownership structure, organisational structure or management structure of the producer or provider of maintenance or support services is not transparent; 10) financing of the producer or provider of maintenance or support services is not transparent; 11) the products or services of the producer or provider of maintenance or support services include vulnerabilities and no adequate security

16. Where hardware or software is found to pose a risk to national security, Paragraph 196⁵ of the ESS lays down certain fixed transitional periods: until 31 December 2025 for 5G technology¹² and until 31 December 2029 for 2G, 3G, and 4G hardware and software.¹³

17. Upon receipt of an application for authorisation for the use of hardware and software in a communications network, the TTJA is obliged, pursuant to Paragraph 87⁴ of the ESS, to request an opinion from the Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu (Cybersecurity Council of the Security Committee of the Government of the Republic of Estonia) ('the KJN') on whether the hardware and software specified in that application poses a risk to national security.

18. By Decision No 1 of 27 October 2022, the KJN identified such a risk in relation to all of the hardware and software at issue.¹⁴ According to the order for reference, that risk was identified in relation to *all* 12 criteria listed in Paragraph 87³(3) of the ESS.¹⁵ That body also proposed that the TTJA grant a usage permit until 31 December 2025 for 5G functionality and until 31 December 2029 for 2G-4G functionality ('the KJN decision').

19. By Decision No 1-7/22-436 of 25 November 2022, the TTJA found that all hardware and software listed in the applicant's application for authorisation posed a risk to Estonia's national security. It therefore issued the applicant a time-limited usage permit until 31 December 2025 for 5G functionality and until 31 December 2029 for 2G-4G functionality, in line with Paragraph 196⁵ of the ESS ('the TTJA decision').

20. By appeal of 1 December 2022, the applicant challenged the KJN's and the TTJA's respective decisions (together, 'the contested decisions') before the

measures have been implemented to eliminate these; 12) the producer or provider of maintenance or support services is not able to secure continued deliveries of products or services, except due to force majeure.'

¹² According to the text of Paragraph 196⁵ of the ESS, this covers '5G [non stand-alone] or a newer generation mobile communications network standard'.

¹³ It is my understanding from the text of Paragraph 196⁵ of the ESS that no future authorisation is issued after 31 December 2025 for 5G technology that has been found to pose a risk to national security, whereas authorisation for the continued use of 2G, 3G, 4G hardware and software, even where a finding of a risk to national security was made, may be applied for after 31 December 2029.

¹⁴ According to Paragraph 87³(2) of the ESS, the hardware or software used in a communications network may jeopardise national security due to the high risk posed by the manufacturer or provider of maintenance or support services (point 1) or due to the risk posed by the technical characteristics or configuration of the hardware or software (point 2).

¹⁵ See footnote 11 above. At the hearing, the Estonian Government explained that examples of the types of risks identified related to the potential for espionage, the illegal use of information and data, and the disruption of important services.

referring court. The applicant *inter alia* argues that the KJN and the TTJA did not demonstrate the existence of a risk to Estonian national security, the likelihood of the alleged risk materialising, or the potential extent of the damage arising from the hardware and software at issue. That party also argues that, by virtue of the short transition period, the contested decisions constitute a retroactive prohibition of the hardware and software at issue that has the consequence of expropriating the applicant of its property. That, in turn, must give rise to compensation. The applicant additionally challenges the validity of the contested decisions on the basis that the law, by virtue of which those decisions were adopted, was not notified to the Commission, and so is incompatible with Directive (EU) 2015/1535 (‘the TRIS Directive’).¹⁶ Finally, it alleges that the contested decisions constitute a restriction to the freedom to provide electronic communications networks and services, as laid down in Article 12(1) of the EECC, and that any restriction to that freedom must be duly justified, which the competent authorities failed to do.

21. The KJN and the TTJA contest those arguments. In essence, they argue that the contested decisions are based on a risk assessment, for the purposes of which the probability and foreseeability of a risk is sufficient. Those decisions fall within the sole competence of Estonia, which is subject only to limited judicial review. The KJN and the TTJA also observe that the transitional period granted in the contested decisions constitute the maximum period permitted by Paragraph 196⁵ of the ESS. Finally, those parties disagree that the contested decisions are incompatible with the TRIS Directive and the EECC.

22. In those circumstances, the Tallinna Halduskohus (Administrative Court, Tallinn) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

- ‘(1) Does a national legislative package (Paragraph 87³(2), (3), (6), (7) and (8), Paragraph 87⁴(1) to (4) and Paragraph 196⁵(1) to (4) of the [ESS]), which, in order to ensure national security, requires a communications company to obtain authorisation for the use of hardware and software in its communications network, fall within the scope of [the EECC]?’
- (2) If the previous question is answered in the affirmative: is Article 1(3)(c) [of the EECC,] in conjunction with Article 4(2) [TEU,] to be interpreted as meaning that the introduction of such restrictions falls within the exclusive competence of the Member State and constitutes a purely national measure to which the provisions of [the EECC] do not apply?’
- (3) If Question 2 is answered in the negative: does a national legislative package (Paragraph 87³(2), (3), (6), (7) and (8), Paragraph 87⁴(1) to (4) and

¹⁶ Directive of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ 2015 L 241, p. 1).

Paragraph 196⁵(1) to (4) of the ESS) that does not allow a communications company to use hardware and software in its communications network without obtaining authorisation from an administrative authority for the use of that hardware and software constitute a restriction on the freedom to provide electronic communications networks and services within the meaning of Article 12(1) [of the EECC]?

- (4) If Question 3 is answered in the affirmative: is such national legislation to be disapplied if it has not been notified to the [Commission] in advance in accordance with Article 12(1) of [the EECC]?
- (5) If Question 2 is answered in the affirmative: is it compatible with Article 36 TFEU and the principle of proportionality for national legislation to require a communications company to obtain authorisation for the use of hardware and software in its communications network in order to ensure national security, and not to require the administrative authority, when assessing the threat posed by high-risk hardware and software: (a) to examine whether the risks associated with the manufacturer are projected onto the specific hardware and software; (b) to assess the functionality, location and importance of the specific hardware and software in the context of the provision of a communications service; and (c) to examine whether the problems associated with the State in which the manufacturer is established are projected onto the manufacturer?
- (6) Where the use of hardware or software that was already present and actively used in the communications network prior to the introduction of the authorisation requirement is authorised for a period shorter than the useful life of that hardware or software and the hardware or software in question was lawfully acquired, does that constitute a deprivation of property for the purposes of the second sentence of Article 17(1) of the Charter of Fundamental Rights of the European Union [(“the Charter”)]?

23. Written observations were submitted to the Court by the applicant, the Czech, Danish, Estonian, Spanish, French, Italian, Finnish and Swedish Governments and the Commission. The applicant, the KJN, the Estonian, Danish, German, Spanish, French, Italian, Finnish and Swedish Governments and the Commission presented oral argument at the hearing that took place on 11 November 2025.

III. Analysis

24. I will organise my analysis as follows.

25. The first two questions of the referring court relate to the scope of application of the EECC. The first question thus asks whether a legislative scheme which requires *ex ante* authorisation for the use of hardware and software in electronic communications networks and services, such as the one introduced by

the ESS, falls within the material scope of the EECC. I will deal with that question in Section III.A. The second question then asks whether such measures are nevertheless excluded from the scope of that directive because they are taken for the reasons of national security. I will deal with that question in Section III.B. My conclusion in relation to both questions is that the EECC applies in the present case.

26. Given that the EECC applies, the third question seeks guidance on whether the contested measures represent a restriction to the freedom to provide electronic communications networks and services within the meaning of Article 12(1) of the EECC. I will respond in the affirmative to that question in Section III.C. That will lead me to the fourth question, which requests an explanation as to whether those measures had to be notified to the Commission and, if so, what consequences result from their non-notification. I will deal with that question in Section III.D.

27. If the national measures at issue constitute a restriction to the freedom to provide electronic communications networks and services, as I believe they do, another important question that arises in this context is whether and, if so, how such measures could be justified. Such a justification is possible under Article 12(1) of the EECC; that provision refers in that respect to Article 52(1) TFEU. The referring court, however, does not seek clarification as to how to conduct the proportionality review under Article 12(1) of the EECC. Instead, it poses that question, in the form of the fifth question, in relation to the free movement of goods, and subject to the proviso that the Court finds that the EECC does not apply. As I will propose that the EECC applies, it will not be necessary to answer the fifth question in the form put to the Court. Nevertheless, the substance of that question is relevant to the referring court for the purposes of the justification under Article 12(1) of the EECC, read in combination with Article 52(1) TFEU. Therefore, instead of answering the fifth question as put to the Court, I will propose to reformulate it as if it were asked in relation to the latter provisions (and not in relation to Articles 34 and 36 TFEU). I will deal with the question thus reformulated under Section III.E.

28. Finally, by its sixth question, the referring court seeks assistance from the Court to determine whether the measures at issue, given the circumstances of the present case, represent a *de facto* deprivation of the applicant's property, in which case it considers that Article 17(1) of the Charter requires that adequate compensation should be provided. Under Section III.F, I will propose to the Court that the measure at issue does not represent such a deprivation, but that it does represent an interference with the use of property, which can, however, be justified and so does not require compensation on the basis of Article 17(1) of the Charter.

A. The first question

29. By its first question, the referring court asks, in essence, whether the relevant provisions of the ESS, on the basis of which the contested measures were taken, fall within the scope of application of the EECC.

30. The positions of the parties that have provided observations in these proceedings differ as to the answers to that question. The applicant, the Estonian and French Governments and the Commission consider, in essence, that the EECC applies to the measures at issue in the present case. The Estonian Government, supported by the Commission, specifically explains that the ESS was, in fact, adopted in implementation of the EECC. Taking the opposing view, the Danish, Czech, Italian, Swedish and Finnish Governments consider, in essence, that the EECC does not apply given that the authorisation measure at issue was taken with a view to protecting Estonia's national security. For its part, the Spanish Government argues that measures adopted to protect national security fall outside of the scope of the EECC, but that that does not dispense the Member States from the obligation to comply with the EECC, which applies in the present case.

31. I consider that the EECC applies and that the measures at issue fall within the scope *ratione materiae* of that directive.

32. The EECC is the principal legislative act in the area of electronic communications. It lays down a harmonised legal framework in order to ensure an internal market in electronic communications networks and services.¹⁷ To achieve that objective, it seeks to remove obstacles relating to the provision of electronic communications networks and services by prohibiting restrictions imposed by the Member States and by adopting common rules.¹⁸

33. That framework applies also to mobile networks, at issue in the present case.¹⁹

34. In principle, therefore, all national rules that concern the regulation of electronic communications networks and services fall within the scope of the EECC.

35. One of the objectives of the EECC is to ensure the security of the internal market of electronic communications networks and services. Thus, according to

¹⁷ See, to that effect, Article 1(1) of the EECC. To that extent, the EECC recasts a number of acts adopted as a package in March 2002 which previously regulated electronic communications with a view of adjusting the regulatory framework to technological and market developments. See, to that effect, judgment of 27 February 2025, *T-2* (C-562/23, EU:C:2025:126, paragraph 37 and the case-law cited).

¹⁸ As recital 5 of the EECC states, the freedom to provide electronic communications networks and services should be subject only to the conditions laid down in that directive.

¹⁹ See Article 2(1) of the EECC.

Article 1(2)(a), that directive aims to ‘implement an internal market in electronic communications networks and services that results in the deployment and take-up of very high capacity networks, sustainable competition, interoperability of electronic communications services, accessibility, *security of networks and services* and end-user benefits’.²⁰

36. To that end, Article 40(1) of the EECC expressly requires Member States to ensure that providers of public or publicly available electronic communications networks or services take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services. Having regard to the state of the art, those measures must ensure ‘a level of security appropriate to the risk presented’, which includes measures capable of preventing and minimising the impact of security incidents on users and other networks and services.

37. National rules adopted for the purpose of achieving the objective of the ‘security of networks and services’ must therefore be seen as falling within the scope of the EECC.

38. The concept of the ‘security of networks and services’ is defined in Article 2(21) of the EECC as ‘the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services’.

39. That definition must be read alongside the definitions of the concepts of ‘electronic communications network’²¹ and ‘electronic communications service’.²²

40. The former of those concepts is worded broadly and covers inter alia the physical equipment necessary for the provision of that network (and thus also hardware and software contained therein).²³ The latter concept refers to the

²⁰ Emphasis added.

²¹ See Article 2(1) of the EECC.

²² See Article 2(4) of the EECC.

²³ The concept of ‘electronic communications network’ is defined in Article 2(1) of the EECC as ‘transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.’

transmission of signals through physical infrastructure, which the Court has interpreted as also extending to the software used, *inter alia*, for internet access.²⁴

41. It follows that the concept of ‘security of networks’, as defined in Article 2(21) of the EECC, should be understood to encompass the security of both *hardware* and *software* elements of an electronic communications network.

42. In order to implement Article 40(1) of the EECC, Article 41(1) thereof requires Member States to ensure that the competent authorities have the power to issue binding instructions, including those relating to the measures required to prevent a security incident from occurring when a ‘significant threat’ has been identified.

43. No further provision is made as to the rules that the Member States must adopt in that respect. Accordingly, EU law leaves to the Member States the decision on how to implement those requirements to ensure the security of their networks and services.

44. In the present case, it follows from the order for reference, the observations of the applicant, and the observations of the Estonian Government and the KJN, confirmed at the hearing, that the rules at issue seek to implement the EECC, and in particular Article 40(1) and Article 41(1) thereof, into Estonian law.

45. There is no reason why an *ex ante* authorisation procedure for the use of hardware and software for the provision of electronic communications networks and services, such as the one required by the ESS, should not be considered as one of the possible design options for the implementation of Article 40(1) and Article 41(1) of the EECC.

46. Nor is that contested in these proceedings.

47. In the light of the above, I propose that the Court answer the first question posed by the referring court in the affirmative, namely that the EECC must be interpreted as covering a national legislative package which, in order to ensure the security of the national electronic communications network and its services, requires that an operator that wishes to provide such a network and service obtain authorisation for the use of hardware and software in its communications network.

B. The second question

48. By its second question, which is made conditional on an affirmative answer to the first question, the referring court seeks guidance, in essence, as to whether the effect of Article 4(2) TEU and Article 1(3)(c) of the EECC is such as to render

²⁴ See, to that effect, judgments of 5 June 2019, *Skype Communications* (C-142/18, EU:C:2019:460, paragraph 49), and of 13 June 2019, *Google* (C-193/18, EU:C:2019:498, paragraphs 34, 35 and 41).

the authorisation measures at issue as falling within the exclusive competence of the Member States to which the EECC does not apply, because those measures were taken with a view to guaranteeing national security.

49. I can be brief on that question.

50. The last sentence of Article 4(2) TEU provides that national security remains the sole responsibility of each Member State. That idea is also reflected in Article 1(3)(c) of the EECC, which provides that that directive is without prejudice to actions taken by the Member States for public order and public security purposes and for defence.

51. Therefore, and despite terminological differences between those two provisions,²⁵ I agree with the Commission and the French Government that Article 1(3)(c) of the EECC in essence constitutes an expression of Article 4(2) TEU.

52. Should these two provisions be read as meaning that measures taken for national security purposes should be excluded from the scope of the EECC?

53. The applicant, the Estonian, Spanish and French Governments and the Commission consider that although the Member States alone may decide on measures designed to protect their national security, that does not relieve them from complying with the EECC. The effect of Article 4(2) TEU and Article 1(3)(c) EECC is therefore not such as to withdraw from the scope of EU law the authorisation measure at issue. Taking the opposing view, the Danish, Czech, Italian, Swedish and Finnish Governments highlight that given the fact that the measures at issue were taken with a view of protecting Estonia's national security, the effect of Article 4(2) TEU and Article 1(3)(c) EECC is such as to exclude the application of EU law.

²⁵ Article 4(2) TEU refers to 'national security', while Article 1(3)(c) of the EECC uses the terms 'public order' and 'public security'. However, for instance, recital 6 of the EECC uses the term 'essential security interests' alongside references to 'public policy' and 'public security', as part of its 'without prejudice' language. Given that there is no indication in the text of the EECC itself, its objective, or its preparatory documents to consider differently (see Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (COM(2016) 590 final/2)), I am of the view that the terminology used in the text of Article 1(3)(c) of the EECC should be read as including the concepts of 'national security' or 'essential security interests'. That would also be in line with the language used in the EECC's predecessor directive, which, in its recitals (albeit without a specific article to that effect), already contained such language. See recital 7 of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ 2002 L 108, p. 33).

54. In my view, the case-law of the Court already explains that Article 4(2) TEU does not exclude national security measures from the reach of EU law.²⁶

55. Rather, that provision confirms that the European Union has no competence to decide what is necessary for and how to protect the security of the Member States. Nevertheless, even if, under Article 4(2) TEU, national security remains the sole responsibility of each Member State, ‘the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from the need to comply with EU law’.²⁷

56. Therefore, even if Estonia adopted the contested legislation with a view to protecting its national security, that does not exclude that legislation and the measures adopted on its basis from the scope of application of the EECC.

57. In other words, where measures adopted for safeguarding national security conflict with EU rules, the public interest of protecting national security may be used to justify that conflict; however, those measures nevertheless have to meet the proportionality test in order to demonstrate that they are lawful. I will come back to that issue when answering the fifth question.

58. In the present proceedings, as I already explained, the Estonian Government specifically takes the position that the legislation at issue protects national security interests, but that it is, at the same time, adopted in implementation of the EECC.²⁸ In fact, in order to justify its national administrative decisions to treat the hardware and software at issue of ‘high risk’ to the security of its telecommunications infrastructure, the Estonian Government relies on certain EU soft law instruments drawn up by the Commission²⁹ and a cooperation group of national securities agencies.³⁰

²⁶ See, for example, judgments of 26 October 1999, *Sirdar* (C-273/97, EU:C:1999:523, paragraph 15); of 6 October 2020, *Privacy International* (C-623/17, EU:C:2020:790, paragraph 44 and the case-law cited); and of 15 July 2021, *Ministrstvo za obrambo* (C-742/19, EU:C:2021:597, paragraph 40 and the case-law cited).

²⁷ See, recently, judgment of 29 July 2024, *protectus* (C-185/23, EU:C:2024:657, paragraph 62 and the case-law cited).

²⁸ In that sense, these proceedings constitute an interesting example of the ‘securitisation’ of EU law. On the development of a ‘security duopoly’ between the Member States and the EU political institutions, where political directions cross-feed into actions at national and EU level, see Pilniok, A., ‘Governance of the European Security Union’, in Dietrich, J.-H. and Pilniok, A., *European Security Union: Law and Policies*, Beck/Hart/Nomos, 2024, pp. 18 and 19.

²⁹ See, inter alia, the 2019 Cybersecurity Recommendation and Communication from the Commission, Implementation of the 5G cybersecurity Toolbox (C(2023) 4049 final) (‘the Communication on the implementation of the 5G Toolbox’).

³⁰ See NIS Cooperation Group, ‘EU coordinated risk assessment of the cybersecurity of 5G networks’, 2019 (‘the Coordinated Risk Assessment’), available at: <https://digital->

59. There is, accordingly, convergence between the *national* security concerns of Estonia and the security requirements laid down at *EU level*.

60. That element distinguishes the present case from the judgment in *Ministrstvo za obrambo*.³¹ In that case, the Court considered that certain categories of military activities fell outside of the scope of Directive 2003/88/EC concerning certain aspects of the organisation of working time³² ‘where those activities are so particular that they are always absolutely incompatible with the requirements imposed by that directive’.³³

61. On the basis of the foregoing, I propose that the Court answer in the negative the second question and find that Article 4(2) TEU and Article 1(3)(c) of the EECC must be interpreted as meaning that a measure requiring the authorisation of hardware and software for the provision of a public or publicly available electronic communications network or service is not excluded from the scope of application of the EECC, even if that measure was adopted with a view to protecting national security interests.

C. The third question

62. It follows from my answers to the first two questions that the ESS and the contested decisions, which were adopted on the basis of the ESS, fall within the scope of application of the EECC. That brings me to the third question.

63. By its third question, the referring court asks, in essence, whether a national measure which requires prior authorisation for the use of hardware and software constitutes a restriction to the freedom to provide electronic communications networks and services, within the meaning of Article 12(1) of the EECC.

64. The applicant considers that that question should be answered in the affirmative. It argues that Article 12(1) of the EECC requires the Member States to guarantee the freedom to provide electronic communications services, which the authorisation procedure in the ESS restricts. The Estonian, Spanish, French and Italian Governments and the Commission disagree with that position. They argue, in essence, that the authorisation procedure laid down in the ESS acts as a

strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security. See also NIS Cooperation Group ‘Cybersecurity of 5G networks, EU Toolbox of risk mitigating measures’, 2020 (‘the 5G Toolbox’), available at: <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>.

³¹ Judgment of 15 July 2021 (C-742/19, EU:C:2021:597).

³² Directive of the European Parliament and of the Council of 4 November 2003 (OJ 2003 L 299, p. 9).

³³ See judgment of 15 July 2021, *Ministrstvo za obrambo* (C-742/19, EU:C:2021:597, paragraph 75).

precondition to the freedom to provide electronic communications services, and not as a restriction, given that the freedom to provide electronic communications services is, under Article 12(1) of the EECC ‘subject to the conditions set out in this Directive’. Given that the security of electronic communications networks and services constitutes one of those conditions, the argument goes, Member States may legitimately lay down an authorisation procedure such as that at issue in the main proceedings.³⁴

65. From those positions, it arises that the Court has two options on how to characterise the authorisation measure at issue under Article 12(1) of the EECC: (i) as a *condition* for the provision of electronic communications networks and services or (ii) as a *restriction* to the provision of those networks and services.

66. I am of the view that such a requirement constitutes a restriction the provision of such networks and services, within the meaning of Article 12(1) of the EECC. However, I consider that restriction to be justified.

67. In this regard, it is worthwhile recalling the first two sentences of Article 12(1) of the EECC:

‘Member States *shall ensure* the freedom to provide electronic communications networks and services, subject to the conditions set out in this Directive. To this end, Member States *shall not prevent* an undertaking from providing electronic communications networks or services, except where this is necessary for the reasons set out in Article 52(1) TFEU.’³⁵

68. In principle, therefore, the baseline arising from that provision is that, subject to certain conditions, the Member States must *allow* undertakings to provide electronic communications networks and services.

69. Moreover, the Member States cannot *prevent* those undertakings from exercising that freedom through any restriction that is not imposed directly by the EECC itself as a condition for the provision of such electronic communications networks and services.

70. While mandating *negative integration* (that is, prohibiting Member State measures that create obstacles to the freedom to provide electronic communications networks and services),³⁶ Article 12(1) of the EECC also

³⁴ The French Government also points out that it is not obvious that a system of prior authorisation for hardware and software, such as that at issue in the main proceedings, affects the possibility of providing such networks or services. In its view, that system in no way requires telecommunications operators to obtain authorisation in order to be able to carry out the activity of providing electronic communications networks and services more generally.

³⁵ Emphasis added.

³⁶ Even though Article 12(1) of the EECC contains wording according to which Member States shall not ‘prevent’ the freedom to provide electronic communications networks and services, I consider that that expression should be understood more broadly as prohibiting Member States

recognises the need for *positive integration* (that is, harmonising the need to ensure security as a condition for the provision of electronic communications networks and services).

71. However, even if requiring that networks and services be secure, positive integration in relation to the security of those networks and services does not happen at the EU level.

72. The EECC does not lay down the measures that guarantee such security. It leaves that choice to the Member States by obliging them, through Article 40(1) and Article 41(1) thereof, to make those choices.

73. In other words, even if, under the EECC, the security of networks and services constitutes a condition for the provision of such networks and services, prior authorisation for the use of hardware and software in their provision is not.

74. The converse, that is to say if any measure that a Member State chooses to ensure the security of networks and services were automatically characterised as a condition for the proper functioning of the internal market in electronic communications networks and services, would mean that the Member States could easily create obstacles to free movement.³⁷

75. That type of automatic exclusion from judicial review as to their proportionality of measures chosen by the Member States would be at odds with the intention of Article 12(1) of the EECC to prevent obstacles to the freedom to provide electronic communications networks and services.

76. Therefore, I propose an interpretation according to which a particular national measure taken with a view to ensuring the security of a Member State's networks and services may still be characterised as a restriction to the freedom to provide such networks and services, prohibited under Article 12(1) of the EECC, even if Member States are required by that directive to ensure the security of their networks.

to impose *any kind of obstacles* to their provision. That follows from the EECC's purpose of establishing an internal market in electronic communications networks and services. That conclusion may also be drawn from the different language versions of Article 12(1) of the EECC, which use expressions meaning both 'hinder' and 'prevent': compare, in that respect, for example, the German-language version, which refers to '*hindern*'; the Spanish-language version, which refers to '*no impedirán*'; the French-language version, which refers to '*n'empêchent pas*'; or the Croatian-language version, which refers to '*ne smiju sprečavati*'.

³⁷ Imagine a situation in which a Member State would decide that, in order to ensure the security of networks, any hardware and software used in such networks must be produced by undertakings established in that State. That type of protectionist measure would clearly be contrary to the freedom to provide networks and services, but would be justifiable if the EECC were construed in such a way as to automatically find acceptable and excluded from further scrutiny any measure adopted with a view to achieving the objective of security of networks and services.

77. Any requirements for prior authorisation to access the internal market are, in principle, considered obstacles to free movement, be it of goods,³⁸ services,³⁹ capital,⁴⁰ or the freedom of establishment.⁴¹ Such a requirement always makes a freedom less attractive and access to relevant markets more difficult.

78. In this regard, it is clear that an *ex ante* authorisation procedure, such as that at issue in the present case, which allows the competent authorities to prohibit the use of certain hardware and software on the ground of their ‘high-risk’ nature, constitutes a measure that, in principle, represents an obstacle to the free movement of electronic communications networks and services given that it is liable to make access to and the exercise of that service less attractive or more difficult.

79. Therefore, such a measure is, in principle, prohibited by Article 12(1) of the EECC.

80. The Estonian legislation at issue is, therefore, liable to restrict the freedom to provide electronic communications networks and services, contrary to the first sentence of Article 12(1) of the EECC.

81. That being said, by virtue of Article 12(1) of the EECC, such a measure may be justified by one of the grounds listed in Article 52(1) TFEU.

82. The resulting proportionality analysis, which encompasses considerations of national security, is a matter for the referring court. It has not asked for guidance on that particular aspect of Article 12(1) of the EECC. That being said, in relation to my proposed answer to the fifth question, I provide guidance which may also be of use to the referring court in that respect.

83. On the basis of the foregoing, I propose that the Court answer the third question in the affirmative: Article 12(1) of the EECC must be interpreted as meaning that a national legislative package that requires authorisation from an administrative authority for the use of hardware and software in the provision of electronic communications networks and services constitutes a restriction to the freedom to provide such networks and services within the meaning of that provision. Such a restriction can be justified by reasons provided for in Article 52(1) TFEU.

³⁸ See, for example, judgment of 23 February 1995, *Bordessa and Others* (C-358/93 and C-416/93, EU:C:1995:54, paragraph 25).

³⁹ See, for example, judgment of 4 December 1986, *Commission v Germany* (205/84, EU:C:1986:463, paragraph 28).

⁴⁰ See, for example, judgment of 14 March 2000, *Église de scientologie* (C-54/99, EU:C:2000:124, paragraph 14).

⁴¹ See, for example, judgment of 1 June 2010, *Blanco Pérez and Chao Gómez* (C-570/07 and C-571/07, EU:C:2010:300, paragraph 54).

D. The fourth question

84. The third sentence of Article 12(1) of the EECC requires that Member States duly reason any limitation to the freedom to provide electronic communications networks and services, and that they notify such a limitation to the Commission.

85. In the light of that provision, the referring court wishes to know, by its fourth question, what consequences ensue from the failure to notify a limitation to the right contained in Article 12(1) of the EECC such as, in the present case, a legislative package requiring *ex ante* authorisation for the use of hardware and software in electronic communications networks. Most importantly, that court asks whether the failure to make such a notification renders such a measure inapplicable.

86. According to the applicant, the legislation at issue was not notified to the Commission. For that reason, the authorisation procedure laid down in the ESS cannot be enforced against it. The Estonian, Spanish, French and Italian Governments and the Commission, joined, at the hearing, also by the TTJA and the German and Finnish Governments, contend that no notification was necessary as, in their view, the authorisation requirement arising from the ESS does not constitute a restriction, but rather a condition imposed by the EECC to provide electronic communications networks and services.

87. Contrary to those positions, as I have already explained in relation to the third question, in my view, an *ex ante* authorisation measure, such as the one introduced in Estonia by the ESS, constitutes a restriction to the freedom to provide electronic communications networks and services. Therefore, to my mind, that type of measure should have been notified to the Commission.

88. However, I wish to observe that it is not clear from the court file whether that measure was indeed notified. According to the Estonian Government, a draft version of the ESS, including the authorisation framework, was communicated to the Commission in 2020,⁴² before it entered into force in 2022. The applicant, however, seeks to contest the existence of such a notification. It is for the referring court to verify whether indeed that was the case.

89. That being said, even if the Estonian Government did not notify the legislative requirement of prior authorisation to the Commission, I am of the view that the failure to do so does not result in the non-applicability of that part of the ESS as regards the applicant, that is, the effect of non-notification is not the same as that which would arise in a case of non-notification of technical requirements under the TRIS Directive.

⁴² The Estonian Government refers to the technical notification of that draft, received by the Commission on 20 October 2020, available at: <https://technical-regulation-information-system.ec.europa.eu/en/notification/15441>.

90. First, the TRIS Directive expressly excludes its application from the area of electronic communications networks and services. Article 1(3) thereof lays down that it ‘shall not apply to rules relating to matters which are covered by Union legislation in the field of telecommunications services, as covered by [the EECC’s predecessor directive]’.

91. For the purposes of the technical rules and standards relating to electronic communications networks and services, the EECC therefore represents *lex specialis* in relation to the TRIS Directive.

92. Second, as the Commission explains, no analogy can be drawn between, on the one hand, a failure to notify under Article 12(1) of the EECC, and, on the other, the non-compliance with the notification procedure put in place by the TRIS Directive and the relevant case-law, according to which non-notification of a technical standard results in its non-applicability towards individuals.⁴³

93. That is because, unlike the TRIS Directive, Article 12(1) of the EECC does not make the applicability of conditions relating to the provision of electronic communications networks and services subject to Commission approval or the elapsing of a minimum time period.

94. Therefore, the failure to notify a limitation to the freedom to provide electronic communications networks and services under Article 12(1) of the EECC does not result in the impossibility to apply the authorisation procedure laid down in the ESS to the applicant.

95. For the above reasons, I propose that the Court respond to the fourth question that the failure to notify to the Commission a limitation to the freedom to provide electronic communications networks, within the meaning of Article 12(1) of the EECC, does not result in the non-applicability of the non-notified national rules.

E. The fifth question

96. The fifth question, as asked, relates to national measures that restrict the free movement of goods, as provided for in Article 34 TFEU, but which may be justified on the basis of Article 36 TFEU. That question was put to the Court under the condition that it finds the EECC not applicable.

97. However, as I have explained, I consider the EECC to be applicable in the present case. In principle, therefore, the Court need not answer the fifth question.

⁴³ See, in particular, judgments of 30 April 1996, *CIA Security International* (C-194/94, EU:C:1996:172, paragraph 54), and of 21 December 2023, *Papier Mettler Italia* (C-86/22, EU:C:2023:1023, paragraph 44).

98. That being said, in substance, the answer to that question as asked would be of use to the referring court for deciding whether the contested measures introduced on the basis of the ESS may be justified under Article 12(1) of the EECC, under which they represent a restriction.

99. As the Court has the possibility to reformulate a question put to it in a way that it considers useful for the resolution of the proceedings before the referring court, I propose that the Court do so in the present case.⁴⁴

100. As reformulated, the fifth question would therefore enquire whether it is compatible with Article 12(1) of the EECC and the principle of proportionality for national legislation to require a communications company to obtain authorisation for the use of hardware and software in its communications network in order to ensure national security, and not to require the administrative authority, when assessing the threat posed by such high-risk hardware and software: (a) to examine whether the risks associated with the manufacturer are projected onto the specific hardware and software; (b) to assess the functionality, location and importance of the specific hardware and software in the context of the provision of a communications service; and (c) to examine whether the problems associated with the State in which the manufacturer is established are projected onto the manufacturer.

101. It is important in that respect to highlight that the referring court does not seek an answer in relation to the proportionality of the contested decisions adopted on the basis of the ESS. Rather, that court seeks guidance on whether the authorisation procedure regulated by the ESS, on which the contested decisions are based, can be justified if it does not impose an obligation on the competent authorities to first assess whether the risk to national security is genuine, before denying the application for authorisation on those grounds. Only if the ESS is found valid from that perspective does the question then arise whether the manner in which it was implemented is proportionate.

102. A measure constituting a restriction to the freedom to provide electronic communications networks and services, within the meaning of Article 12(1) of the EECC, may be justified for the reasons set out in Article 52(1) TFEU, that is to say public policy, public security and public health.

103. In the present case, the Estonian Government justifies the limitation introduced by the ESS on the ground of national security (in the sense of the security of its telecommunications infrastructure), and on the ground that those measures implement the EECC, more particularly its Article 40(1) and Article 41(1).

⁴⁴ See, *ex multis*, judgment of 15 July 2021, *Ministrstvo za obrambo* (C-742/19, EU:C:2021:597, paragraph 31 and the case-law cited).

104. It is not disputed that security of communications networks is of considerable importance in contemporary democratic societies: a secure and trustworthy telecommunications infrastructure is not only necessary for the effective exercise of a number of EU values and fundamental rights, including the value of democracy and the freedom of expression, it also ensures social stability given that the influence over, or the disruption to, a Member States' telecommunications infrastructure may affect other sectors of the economy and everyday life of EU citizens more generally.⁴⁵

105. I also observe that the Court has already recognised that the security of a Member State's telecommunications infrastructure may constitute an element of a State's public security.⁴⁶

106. Moreover, the EEC pursues the objective of ensuring the security of electronic communications networks and services, and, to that end, by virtue of Article 40(1) and Article 41(1), mandates that the Member States ensure the security of their electronic communications networks and services.⁴⁷

107. However, even if the security of a Member States' electronic communications network and its services is recognised as a fundamental interest of society at both Member States and EU level, and can therefore be relied upon as a justification to restrict the freedom to provide such networks and services, that restriction may be imposed only if the risk to that interest is genuine, present and sufficiently serious in the particular case.⁴⁸

108. In that respect, a Member State cannot justify such a restriction merely by invoking reasons of national security.⁴⁹

⁴⁵ See, in that respect, recitals 5 and 37 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ 2022 L 333, p. 80) ('the NIS 2 Directive').

⁴⁶ See, to that effect, judgment of 20 June 2002, *Radiosistemi* (C-388/00 and C-429/00, EU:C:2002:390, paragraph 44). In any event, already since the judgment of 10 July 1984, *Campus Oil and Others* (72/83, EU:C:1984:256, in particular paragraphs 34 to 36), it is clear that the case-law understands the concept of public security as transcending law and order and the use of the police forces and the military; therein, the Court held that that concept may also attach to other kinds of threats to a Member State's institutions, its essential public services, and the needs of society more generally.

⁴⁷ See points 32 to 42 of this Opinion.

⁴⁸ See, *ex multis*, judgments of 14 March 2000, *Église de scientologie* (C-54/99, EU:C:2000:124, paragraph 17 and the case-law cited), and of 18 June 2020, *Commission v Hungary (Transparency of associations)* (C-78/18, EU:C:2020:476, paragraph 91 and the case-law cited).

⁴⁹ See, by analogy, judgment of 3 September 2008, *Kadi and Al Barakaat International Foundation v Council and Commission* (C-402/05 P and C-415/05 P, EU:C:2008:461,

109. Instead, the legislation permitting such a restriction, in this case the ESS, must oblige the competent authorities, in the present case the TTJA and the KJN, to assess whether the particular equipment at issue genuinely represents such a risk to the security of the national telecommunications network.

110. While that assessment may be different for risks emanating from third States or their suppliers,⁵⁰ it cannot be based on a general suspicion;⁵¹ instead, it must involve a specific assessment of the use for which that equipment is intended and the risks associated therewith. That analysis may involve, for example, risks related to the type of equipment at issue, the manufacturer of that equipment, or the State within which that manufacturer is established.⁵²

111. In that light, the fifth question of the referring court should be answered in the sense that Article 12(1) of the EECR requires that national legislation imposing a requirement for the prior authorisation for the use of hardware and software with a view to protecting the security of electronic communications networks and services oblige the bodies empowered to decide on whether to grant such an authorisation to assess whether the hardware and software at issue, the use of which is requested, presents a genuine risk to the security of the network, which may include taking into consideration the use for which such equipment is intended, whether the risks associated with the State in which the manufacturer is established are projected onto the manufacturer, and whether the risks associated with the manufacturer are projected onto the specific hardware and software.

112. It is my understanding, which is for the referring court to verify, that the ESS lays down precise criteria on the basis of which the competent national authorities may conclude that there exists a risk to national security. For that purpose, it appears that account is taken, *inter alia*, of the existence of a threat relating to the manufacturer and the third country in which that manufacturer is established.⁵³

113. When reviewing the contested decisions, the national court will have to assess whether those criteria were indeed taken into consideration when assessing

paragraph 343) (explaining that a measure cannot escape all review by the EU Courts simply because the act laying them down concerns national security).

⁵⁰ See, by analogy, judgment of 26 February 2019, *X (Controlled companies established in third countries)* (C-135/17, EU:C:2019:136, paragraph 90 and the case-law cited).

⁵¹ See, to that effect, judgments of 14 March 2000, *Église de scientologie* (C-54/99, EU:C:2000:124, paragraph 22), and of 18 June 2020, *Commission v Hungary (Transparency of associations)* (C-78/18, EU:C:2020:476, paragraphs 86 and 93).

⁵² See, by analogy, judgment of 10 March 2016, *Safe Interenvíos* (C-235/14, EU:C:2016:154, paragraph 104) (explaining that, in the realm of money laundering, an assessment of the high-risk nature of a customer may involve the type of customer, the country, the product, or the transaction at issue).

⁵³ See, in that respect, footnote 11 above.

the risks in the particular situation of the case at hand, leading to the temporal limitation of the usage permit.

114. Given that it involves deep knowledge of the technical, political and security aspects linked to a particular situation, the assessment of the existence of a risk in relation to a specific manufacturer, its equipment, or the use of that equipment cannot be made by the EU Courts. Nevertheless, when a national court is requested to review measures by which the use of certain hardware and software is prohibited on grounds of national security, the competent authorities must be able to provide reasonable explanations as to the grounds for the finding of such a risk;⁵⁴ where necessary, that may require the use of different judicial techniques.⁵⁵

115. Where, as in the present case, there is convergence between the security interests at issue at EU and national level, a national court may also take into consideration – in the course of the judicial review of the measure at issue – risk assessments undertaken by the EU institutions and bodies as well as by national bodies.

116. In that respect, a number of documents relied upon by the Estonian Government might be relevant for the referring court's assessment: that government, *inter alia*, refers to the Commission's 2019 Cybersecurity Recommendation, the Coordinated Risk Assessment and the 5G Toolbox⁵⁶ by the NIS Cooperation Group⁵⁷ and the Commission's Communication on the implementation of the 5G Toolbox.

117. While those documents constitute elements of soft law not binding on the Member States, they lay down a coordinated risk assessment by the competent authorities at national and EU level, on the basis of which the Commission *inter alia* identified the equipment produced by the manufacturer of the hardware and software at issue as presenting 'materially higher risks than other 5G suppliers'

⁵⁴ See, by analogy, judgment of 21 November 1991, *Technische Universität München* (C-269/90, EU:C:1991:438, paragraphs 13 and 14).

⁵⁵ See, to that effect, judgment of 4 June 2013, *ZZ* (C-300/11, EU:C:2013:363, paragraph 57 and the case-law cited).

⁵⁶ That toolbox results from one of the objectives laid down by the Commission in the Cybersecurity Recommendation (see point 1(c) thereof), which lays down that the NIS Cooperation Group 'identify a possible common set of measures to be taken to mitigate cybersecurity risks related to infrastructures underpinning the digital ecosystem, in particular 5G networks'.

⁵⁷ See footnote 30 above. That group constitutes a committee established on the basis of Article 11(1) of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ 2016 L 194, p. 1). That directive has, in the meantime, been replaced by the NIS 2 Directive, but the committee continues to exist (see Article 14(1) of the NIS 2 Directive).

and that, by virtue of ‘these high risks ... the Commission considers that decisions adopted by Member States to restrict or exclude Huawei [...] are justified and compliant with the 5G Toolbox’.⁵⁸

118. According to the Communication on the implementation of the 5G Toolbox, that conclusion is based *inter alia* on the fact that there exists a ‘link between [that] supplier and a government of a given third country, the third country’s legislation, and characteristics of the supplier’s corporate ownership.’⁵⁹

119. The Estonian Government explains that its competent authorities took account of that assessment, and that, by virtue of that common identification of risk at both EU and Member State level, they considered that it was necessary to limit exposure to equipment from *inter alia* Huawei, the supplier of the hardware and software at issue, in the provision of electronic communications networks and services.

120. Accordingly, it seems reasonable to me to conclude that the ESS and the contested decisions, which were adopted on its basis, despite constituting a restriction to the freedom to provide electronic communications networks and services, pursue a legitimate objective: that of the prevention of a genuine risk for the security of networks. That, however, is for the referring court to assess.

F. The sixth question

121. It arises from the national file that the hardware and software at issue was used by the applicant for 2G-4G functionality for the provision of electronic communications networks and services prior to the contested decisions. It also arises from the applicant’s explanations that it had procured equipment for 5G functionality with a view to including that equipment in its edge network prior to the introduction of the authorisation requirement in the ESS. Finally, it arises from the referring court’s order and the parties’ explanations that the contested decisions allowed for the use of the hardware and software at issue for a period shorter than the useful life of that equipment.

122. In that respect, by its sixth question, the referring court asks whether, taking into consideration those circumstances, the contested decisions result in a deprivation of property within the meaning of the second sentence of Article 17(1) of the Charter, in which case the applicant might be entitled to adequate compensation.

123. The applicant considers that to be the case. It argues that the authorisation regime at issue results in an unjustified deprivation of property. It also considers

⁵⁸ See Communication on the implementation of the 5G Toolbox, p. 2.

⁵⁹ See Communication on the implementation of the 5G Toolbox, p. 1. For similar supplier-specific vulnerability criteria, see also p. 42 of the 5G Toolbox.

that a sudden change in the legislative regime governing the use of the hardware and software at issue, which introduces a requirement for usage authorisation and results in the prohibition of the use of hardware and software which the applicant legally acquired from a particular manufacturer, is precluded by Article 17(1) of the Charter, unless provision is made for fair and adequate compensation.

124. According to the Commission and the Estonian, Spanish, German, French, Italian, Swedish and Finnish Governments, the framework surrounding the authorisation measure at issue constitutes a type of regulation of the use of property within the meaning of the third sentence of Article 17(1) of the Charter. Accordingly, the contested decisions did not bring about a deprivation of the applicant's ownership in the hardware and software at issue, be that *de facto* or *de jure*. Those parties further consider that said regulation of property in the light of Estonia's national and public security concerns constitutes a proportionate restriction of that right given that the Estonian authorities have provided for a sufficiently long transition period.

125. Under Article 17(1) of the Charter, 'everyone has the right to own, use, dispose of and bequeath his or her lawfully acquired possessions. No one may be deprived of his or her possessions, except in the public interest and in the cases and under the conditions provided for by law, subject to fair compensation being paid in good time for their loss. The use of property may be regulated by law in so far as is necessary for the general interest.'

126. The Court has found that provision to contain three distinct rules. It has explained that 'the first rule, which appears in the first sentence of that provision, is of a general nature and gives concrete expression to the principle of respect for property. The second rule, set out in the second sentence of that provision, refers to a person being deprived of property and makes that deprivation subject to certain conditions. The third rule, which is contained in the third sentence of that provision, recognises that the Member States have the power to regulate the use of property in so far as is necessary for the general interest. Those rules are not, however, unrelated to each other. Indeed, the second and third rules relate to specific examples of infringements of the right to property and are to be interpreted in the light of the principle enshrined in the first rule.'⁶⁰

127. It also follows from the Court's case-law that the protection afforded by Article 17(1) of the Charter is broad and covers, alongside assets with an economic value, the interests associated with the exploitation of a licence or usage permit.⁶¹

⁶⁰ See judgment of 10 July 2025, *INTERZERO and Others* (C-254/23, EU:C:2025:569, paragraph 144 and the case-law cited). See, to that effect, also judgment of 5 May 2022, *BPC Lux 2 and Others* (C-83/20, EU:C:2022:346, paragraph 38 and the case-law cited).

⁶¹ See, to that effect, judgment of 10 July 2025, *INTERZERO and Others* (C-254/23, EU:C:2025:569, paragraphs 145 and 146 and the case-law cited).

128. In the main proceedings, the contested decisions concern an application for the authorisation to use certain hardware and software in the provision of electronic communications networks and services. That application was granted only in part and up until the maximum possible period laid down in the ESS, that is, until 31 December 2029 for 2G-4G functionality and until 31 December 2025 for 5G functionality.

129. Consequently, since there was no interference with the essence of that property, the applicant was not deprived of it.⁶² Instead, the contested decisions constitute a limitation of the use of the applicant's property within the meaning of the third sentence of Article 17(1) of the Charter.⁶³

130. In such a case, the applicant is, in principle, not entitled to compensation.

131. That being said, the limitation of the use of property is possible only in so far as is necessary for the general interest. For the purposes of the present case, that assessment will be similar to that required to justify an interference with the freedom to provide electronic communications networks and services under Article 12(1) of the EECC.

132. However, the referring court did not request any guidance on how to conduct such a proportionality assessment.

133. I might nonetheless observe that one aspect that the referring court should take into consideration in the present case is whether the duration of the period during which the applicant was authorised to continue using the hardware and software at issue, placed in the context of the duration of the period allowing the applicant to prepare for such a regulatory change, was sufficient.

134. That is because the authorisation measure at issue, coupled with strict maximum usage periods, considerably affects investments taken prior to the introduction of those legislative changes.⁶⁴

135. Accordingly, the referring court must assess whether the entirety of the period of time during which the applicant could have prepared to adapt itself to

⁶² See, to that effect, judgment of 10 September 2024, *Neves 77 Solutions* (C-351/22, EU:C:2024:723, paragraphs 82 and 88 and the case-law cited).

⁶³ See, by analogy, judgment of 10 July 2025, *INTERZERO and Others* (C-254/23, EU:C:2025:569, paragraph 146 and the case-law cited) (explaining that 'interests associated with the exploitation of a licence constitute property interests attracting the protection of that Article 1 of Protocol No 1 [to the European Convention for the Protection of Human Rights and Fundamental Freedoms]', so that 'the revocation by operation of law of a licence entitling its holder to pursue an economic activity amounts to a limitation of the right to property guaranteed by that article which, as a measure controlling the use of property, comes within the second paragraph of that article').

⁶⁴ See, to that effect, judgment of 10 July 2025, *INTERZERO and Others* (C-254/23, EU:C:2025:569, paragraph 155 and the case-law cited).

the new legal situation, from the point in time at which the relevant amendments to the ESS were proposed to the end of maximum usage period of the hardware and software at issue, was of sufficient length. If it finds that this was not so, a system of reasonable compensation for the damage suffered should be considered.⁶⁵

136. Finally, when assessing the proportionality of the contested decisions, the referring court should take account of the seriousness of the interference with the fundamental right at issue and the importance of the objective pursued⁶⁶ as well as other interests, such as the interests of recipients of electronic communications networks and services in the safety and security of those networks and services, and the market risk that a prudent and circumspect competitor active on the same market would have assumed as regards the hardware and software at issue.⁶⁷

137. If the referring court finds that the burden placed on the applicant was disproportionately heavy, even if necessary, it might, as explained, be appropriate to have recourse to a fair compensation.

138. On the basis of the foregoing considerations, I propose that the Court answer the sixth question by finding that a limitation of the use of hardware or software that was already present in an electronic communications network prior to the introduction of a usage authorisation requirement, pursuant to which usage is granted for a period shorter than the useful life of that hardware or software, does not constitute a deprivation of property within the meaning of the second sentence of Article 17(1) of the Charter.

IV. Conclusion

139. I propose that the Court answer the questions put to it by the Tallinna Halduskohus (Administrative Court, Tallinn, Estonia) as follows:

- (1) Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code

must be interpreted as covering a national legislative package which, in order to ensure the security of the national electronic communications network and its services, requires that an operator that wishes to provide

⁶⁵ See, to that effect, judgment of 10 July 2025, *INTERZERO and Others* (C-254/23, EU:C:2025:569, paragraphs 155 to 156 and the case-law cited).

⁶⁶ See, most recently, judgment of 18 December 2025, *Slagelse Almennyttige Boligselskab, Afdeling Schackenborgvænge* (C-417/23, EU:C:2025:1017, paragraph 168 and the case-law cited).

⁶⁷ See, to that effect, judgment of 10 July 2025, *INTERZERO and Others* (C-254/23, EU:C:2025:569, paragraph 158 and the case-law cited).

such a network and service obtain authorisation for the use of hardware and software in its communications network.

(2) Article 4(2) TEU and Article 1(3)(c) of Directive 2018/1972

must be interpreted as meaning that a measure requiring the authorisation of hardware and software for the provision of a public or publicly available electronic communications network or service is not excluded from the scope of application of Directive 2018/1972, even if that measure was adopted with a view to protecting national security interests.

(3) Article 12(1) of Directive 2018/1972

must be interpreted as meaning that a national legislative package that requires authorisation from an administrative authority for the use of hardware and software in the provision of electronic communications networks and services constitutes a restriction to the freedom to provide such networks and services within the meaning of that provision.

Such a restriction can be justified by reasons provided for in Article 52(1) TFEU.

(4) Article 12(1) of Directive 2018/1972

must be interpreted as meaning that the failure to notify to the European Commission a limitation to the freedom to provide electronic communications networks does not result in the non-applicability of the non-notified national rules.

(5) Article 12(1) of Directive 2018/1972 and the principle of proportionality

must be interpreted as requiring that national legislation imposing a requirement for the prior authorisation for the use of hardware and software with a view to protecting the security of electronic communications networks and services oblige the bodies empowered to decide on whether to grant such an authorisation to assess whether the hardware and software at issue, the use of which is requested, presents a genuine risk to the security of the network, which may include taking into consideration the use for which such equipment is intended, whether the risks associated with the State in which the manufacturer is established are projected onto the manufacturer, and whether the risks associated with the manufacturer are projected onto the specific hardware and software.

(6) A limitation of the use of hardware or software that was already present in an electronic communications network prior to the introduction of a usage authorisation requirement, pursuant to which usage is granted for a period shorter than the useful life of that hardware or software, does not constitute a

deprivation of property within the meaning of the second sentence of Article 17(1) of the Charter of Fundamental Rights of the European Union.