Edizione provvisoria

CONCLUSIONI DELL'AVVOCATA GENERALE
TAMARA ĆAPETA
presentate il 19 marzo 2026 (1)

Causa C-354/24

Elisa Eesti AS
contro
Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu,
Tarbijakaitse ja Tehnilise järelevalve Amet

[Domanda di pronuncia pregiudiziale proposta dal Tallinna Halduskohus (Tribunale amministrativo di Tallinn, Estonia)]

« Rinvio pregiudiziale – Servizi di telecomunicazione – Direttiva (UE) 2018/1972 – Articolo 40, paragrafo 1, e articolo 41, paragrafo 1 – Sicurezza delle reti e dei servizi – Funzionalità 5G – Procedura di autorizzazione – Fornitori di hardware e software "ad alto rischio" – Divieto di hardware e software "ad alto rischio" per ragioni di sicurezza nazionale – Articolo 4, paragrafo 2, TUE – Articolo 17, paragrafo 1, della Carta – Proporzionalità – Intensità del controllo – Misure positive in caso di influenza o controllo da parte di un paese terzo »

I. Introduzione

1. In che modo le misure adottate da uno Stato membro per tutelare la sicurezza nazionale interagiscono con la normativa dell'Unione adottata per garantire il funzionamento del mercato interno delle reti e dei servizi di comunicazione elettronica?

2. Soprattutto, tali misure nazionali sono escluse dall'ambito di applicazione della direttiva (UE) 2018/1972 (codice europeo delle comunicazioni elettroniche; in prosieguo: il «CECE») (2), in quanto adottate per motivi di sicurezza nazionale, e pertanto sottratte al sindacato giurisdizionale sulla proporzionalità alla luce del diritto dell'Unione?

3. Tali interrogativi sorgono nell'ambito di una normativa adottata in Estonia al fine di istituire una procedura di autorizzazione *ex ante* per l'uso di hardware e software nella fornitura di reti e servizi di comunicazione elettronica. La procedura in parola consente alle autorità competenti di vietare l'uso di determinate apparecchiature qualora siano considerate un rischio per la sicurezza nazionale.

4. La ricorrente nel procedimento principale, la Elisa Eesti AS (in prosieguo: la «ricorrente»), una società figlia della società finlandese di telecomunicazioni Elisa Oyj, è uno dei tre fornitori di reti e di servizi di telecomunicazione mobile a livello nazionale in Estonia. Dinanzi al Tallinna Halduskohus (Tribunale amministrativo di Tallinn, Estonia), giudice del rinvio, essa contesta una decisione con la quale le autorità estoni competenti le hanno negato un'autorizzazione all'uso, nella sua rete di telecomunicazioni, di taluni hardware e software 2G-4G e 5G. Detta decisione è stata adottata in particolare a causa del fatto che tali apparecchiature erano prodotte da una società cinese di telecomunicazioni, la Huawei Corporation (in prosieguo: la «Huawei»), che le autorità estoni hanno considerato un fornitore «ad alto rischio» di tali apparecchiature.

II. Contesto giuridico e fattuale del caso di specie e questioni pregiudiziali

A. Informazioni generali sulle infrastrutture e sulle tecnologie di telecomunicazione 5G

5. La comprensione del contesto della presente causa richiede un livello minimo di spiegazione dell'infrastruttura sottesa alla funzionalità 5G. È da qui che muoverò le mosse.

6. Una rete di telecomunicazioni mobili si compone tradizionalmente di due parti. La prima parte, centrale, di tale infrastruttura è *la rete principale*. Essa contiene l'apparecchiatura centrale che controlla l'intera rete ed è concepita come il canale principale di interconnessione di tutti i punti finali del traffico, aggregando e trasferendo il traffico di rete ad alta velocità (3). La seconda parte di tale infrastruttura è *la rete radio mobile*. Quest'ultima è composta da stazioni di base che dividono una zona di servizio più ampia in «celle» e alle quali i dispositivi cellulari, come i telefonini, possono collegarsi tramite rete mobile di uno Stato membro (4). Tale parte della rete mobile è talvolta denominata «perimetro» di rete.

7. La tecnologia delle telecomunicazioni è definita dalle «generazioni». 2G, 3G e 4G sono generazioni successive di tecnologia di rete mobile non analogica. La quinta generazione di tale tecnologia, ossia il 5G, è destinata a sostituire in futuro l'attuale standard 4G (5). La tecnologia 5G è caratterizzata da velocità e capacità di dati elevate e da una minore latenza (ritardo).

8. La Commissione europea considera la tecnologia 5G una componente importante della realizzazione di reti a banda larga e ad alta capacità nell'Unione europea, nell'interesse dell'economia e della società nel suo complesso (6).

9. Come risulta dalla decisione di rinvio e dal fascicolo nazionale, la tecnologia 5G può essere suddivisa in funzionalità 5G «non autonoma» (*non-stand-alone*) e funzionalità 5G «autonoma» (*stand-alone*). Il 5G *non autonomo* è la tecnologia costruita in aggiunta allo strato di rete esistente dell'infrastruttura 2G-4G (7). La comunicazione avviene quindi ancora da e verso la rete di comunicazione «perimetrale» e «principale». Le reti 5G *autonome* creano una propria rete radio e non dipendono quindi dall'infrastruttura 2G-4G «più vecchia», né dalla rete principale. Gli apparecchi autonomi 5G costituiscono quindi una propria infrastruttura di rete indipendente senza passare previamente attraverso la rete principale. Su questa base, possono comunicare direttamente tra loro senza passare attraverso il «nucleo» dell'infrastruttura di telecomunicazioni. Grazie a tale caratteristica, la tecnologia del 5G autonomo sarà in grado di connettere nell'«Internet delle cose» molti più dispositivi di quanto non fosse possibile in precedenza (8).

10. Dalla decisione di rinvio e dal fascicolo risulta che la rete principale della ricorrente è composta da hardware e software prodotti dalla società svedese Telefonaktiebolaget LM Ericsson (in prosieguo: la «Ericsson») e dalla società finlandese Nokia Corporation (in prosieguo: la «Nokia»), e che la sua rete radiomobile è composta da hardware e software prodotti della società cinese Huawei.

11. La presente controversia riguarda solo la rete radiomobile della ricorrente, vale a dire il perimetro di rete.

B. Contesto normativo e di fatto del procedimento principale

12. Il 23 marzo 2022 (9), la ricorrente ha presentato al Tarbijakaitse ja Tehnilise järelevalve Amet (Ufficio per la protezione dei consumatori e la supervisione tecnica; in prosieguo: il «TTJA») una richiesta di autorizzazione d'uso, nel suo perimetro di rete, i) dell'hardware e del software 2G-4G della Huawei ivi già presenti, e ii) dell'hardware e del software 5G della Huawei da introdurvi a decorrere dal 1º giugno 2022 (in prosieguo, congiuntamente, gli «hardware e software di cui trattasi»).

13. Tale richiesta è stata depositata sulla base dell'elektroonilise side seadus (ESS) (legge estone relativa alle comunicazioni elettroniche) (10). Il giudice del rinvio spiega che l'ESS, tra l'altro, recepisce il CECE.

14. Il capo 8 dell'ESS stabilisce alcuni requisiti per la fornitura di servizi di comunicazione elettronica in Estonia. L'articolo 87^2, paragrafo 1, ivi contenuto, impone alle imprese di comunicazione di adottare misure tecniche e organizzative adeguate a gestire i rischi relativi alla sicurezza e all'integrità di un servizio e di una rete di comunicazione. L'articolo 87^3, paragrafo 1, dell'ESS impone che l'hardware e il software utilizzati nella fornitura di servizi di comunicazione in una rete di comunicazione non costituiscano un rischio per la sicurezza nazionale. Di conseguenza, come prescritto dall'articolo 87^3, paragrafo 6, della medesima legge, un'impresa di comunicazione è obbligata a chiedere al TTJA un'autorizzazione d'uso di hardware o software in una rete di comunicazione.

15. A norma dell'articolo 87^3, paragrafo 2, dell'ESS, un rischio per la sicurezza nazionale si determina sulla base del rischio elevato rappresentato dal produttore o dal fornitore di servizi di manutenzione o di assistenza (punto 1) o a causa del rischio derivante dalle caratteristiche tecniche o dalla configurazione dell'hardware o del software (punto 2). L'elevato rischio rappresentato da un produttore o fornitore di servizi di manutenzione o di assistenza è valutato sulla base di 12 criteri, stabiliti all'articolo 87^3, paragrafo 3, dell'ESS (11).

16. Qualora si riscontri che l'hardware o il software comportano un rischio per la sicurezza nazionale, l'articolo 196^5 dell'ESS stabilisce alcuni periodi fissi transitori: fino al 31 dicembre 2025 per la tecnologia 5G (12) e fino al 31 dicembre 2029 per hardware e software 2G, 3G e 4G (13).

17. Al ricevimento di una richiesta di autorizzazione d'uso di hardware e software in una rete di comunicazioni, il TTJA è tenuto, ai sensi dell'articolo 87^4 dell'ESS, a richiedere un parere del Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu (Consiglio per la cibersicurezza del comitato per la sicurezza del governo della Repubblica di Estonia; in prosieguo: il «KJN») sull'eventuale rischio per la sicurezza nazionale rappresentato dall'hardware e dal software oggetto di tale domanda.

18. Con la decisione n. 1 del 27 ottobre 2022, il KJN individuava un siffatto rischio per tutti gli hardware e software di cui trattasi (14). Secondo la decisione di rinvio, tale rischio era individuato alla luce di *tutti* i 12 criteri elencati all'articolo 87^3, paragrafo 3, dell'ESS (15). Tale organismo inoltre proponeva al TTJA di rilasciare un permesso d'uso fino al 31 dicembre 2025 per la funzionalità 5G e fino al 31 dicembre 2029 per la funzionalità 2G-4G (in prosieguo: la «decisione del KJN»).

19. Con decisione n. 1-7/22-436 del 25 novembre 2022, il TTJA ha constatato che tutti gli hardware e software elencati nella richiesta di autorizzazione della ricorrente presentavano un rischio per la sicurezza nazionale dell'Estonia. Esso ha quindi rilasciato alla ricorrente un permesso d'uso limitato nel tempo fino al 31 dicembre 2025 per la funzionalità 5G e fino al 31 dicembre 2029 per la funzionalità 2G-4G, conformemente all'articolo 196^5 dell'ESS (in prosieguo: la «decisione del TTJA»).

20. Con ricorso del 1º dicembre 2022, la ricorrente ha impugnato le rispettive decisioni del KJN e del TTJA (in prosieguo, congiuntamente: le «decisioni impugnate») dinanzi al giudice del rinvio. La ricorrente sostiene, in particolare, che il KJN e il TTJA non avrebbero dimostrato l'esistenza di un rischio per la

sicurezza nazionale estone, la probabilità della concretizzazione del rischio asserito, o la potenziale portata del danno derivante dagli hardware e software di cui trattasi. Detta parte sostiene altresì che, a causa del breve periodo transitorio, le decisioni impugnate rappresenterebbero un divieto retroattivo degli hardware e software di cui trattasi, con la conseguenza di espropriare la ricorrente dei suoi beni. Ciò dovrebbe, a sua volta, dar luogo a un'indennità. La ricorrente contesta inoltre la validità delle decisioni impugnate in quanto la legge in forza della quale tali decisioni sono state adottate non sarebbe stata notificata alla Commissione, cosicché essa risulterebbe incompatibile con la direttiva (UE) 2015/1535 (in prosieguo: la «direttiva TRIS») (16). Infine, essa afferma che le decisioni impugnate costituirebbero una limitazione della libertà di fornire reti e servizi di comunicazione elettronica, quale prevista all'articolo 12, paragrafo 1, del CECE, e che qualsiasi limitazione di tale libertà dovrebbe essere debitamente giustificata, cosa che le autorità competenti avrebbero omesso di fare.

21. Il KJN e il TTJA contestano tali argomenti. In sostanza, essi sostengono che le decisioni impugnate si baserebbero su una valutazione del rischio, ai fini della quale risulterebbe sufficiente la probabilità e prevedibilità di un rischio. Tali decisioni rientrerebbero nella competenza esclusiva dell'Estonia, soggetta solo a un controllo giurisdizionale limitato. Il KJN e il TTJA rilevano altresì che il periodo transitorio concesso nelle decisioni impugnate costituirebbe la durata massima autorizzata dall'articolo 196^5 dell'ESS. Infine, tali parti non concordano sull'incompatibilità delle decisioni impugnate con la direttiva TRIS e con il CECE.

22. In tale contesto, il Tallinna Halduskohus (Tribunale amministrativo di Tallinn) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se un insieme di disposizioni legislative e regolamentari nazionali (articolo 87^3, paragrafi 2, 3, 6, 7 e 8, articolo 87^4, paragrafi da 1 a 4, nonché articolo 196^5, paragrafi da 1 a 4, [dell'ESS]), le quali impongono a un'impresa di comunicazioni di ottenere un'autorizzazione d'uso di hardware e software nella propria rete di comunicazione al fine di garantire la sicurezza nazionale, rientri nell'ambito di applicazione [del CECE].

2) In caso di risposta affermativa alla precedente questione: se l'articolo 1, paragrafo 3, lettera c), [del CECE,] in combinato disposto con l'articolo 4, paragrafo 2, [TUE,] debba essere interpretato nel senso che l'introduzione di tali restrizioni rientra nella competenza esclusiva dello Stato membro e costituisce una misura puramente nazionale alla quale non si applicano le disposizioni [del CECE].

3) In caso di risposta negativa alla [seconda] questione: se un insieme di disposizioni legislative e regolamentari nazionali (articolo 87^3, paragrafi 2, 3, 6, 7 e 8, articolo 87^4, paragrafi da 1 a 4, nonché articolo 196^5, paragrafi da 1 a 4, dell'ESS) che non consente a un'impresa di comunicazione di utilizzare hardware e software nella propria rete di comunicazione senza il previo ottenimento dell'autorizzazione di un'autorità amministrativa per il suo uso costituisca una limitazione della libertà di fornire reti e servizi di comunicazione elettronica ai sensi dell'articolo 12, paragrafo 1, [del CECE].

4) In caso di risposta affermativa alla [terza] questione: se tali disposizioni debbano essere disapplicate qualora non siano state oggetto di una previa comunicazione alla [Commissione] ai sensi dell'articolo 12, paragrafo 1, [del CECE].

5) Nel caso in cui venga fornita una risposta affermativa alla [seconda] questione: se sia compatibile con l'articolo 36 TFUE e con il principio di proporzionalità il fatto che, al fine di garantire la sicurezza nazionale, le disposizioni legislative e regolamentari nazionali impongano a un'impresa di comunicazione di ottenere un'autorizzazione d'uso di hardware e software nella propria rete di comunicazione e non obblighino l'autorità amministrativa, in sede di valutazione della minaccia derivante da hardware e software ad alto rischio: (a) ad esaminare se i rischi associati al produttore si riflettano sugli specifici hardware e software, (b) a valutare la funzionalità, l'ubicazione e la rilevanza degli specifici hardware e software nell'ambito della fornitura di un servizio di comunicazione, e (c) a verificare se i problemi associati allo Stato di stabilimento del produttore possano riverberarsi su quest'ultimo.

6) Se il fatto che l'autorizzazione d'uso di hardware o software preesistenti all'introduzione del rispettivo obbligo e attivamente utilizzati nella rete di comunicazione venga concessa per un periodo inferiore alla vita utile di hardware o software che, a loro volta, siano stati legittimamente acquisiti, costituisca una privazione della proprietà ai sensi dell'articolo 17, paragrafo 1, seconda frase, della Carta dei diritti fondamentali dell'Unione europea [(in prosieguo: la «Carta»)]».

23. Hanno presentato osservazioni scritte dinanzi alla Corte la ricorrente, i governi ceco, danese, estone, spagnolo, francese, italiano, finlandese e svedese, nonché la Commissione. La ricorrente, il KJN, i governi estone, danese, tedesco, spagnolo, francese, italiano, finlandese e svedese nonché la Commissione hanno svolto osservazioni orali all'udienza tenutasi l'11 novembre 2025.

III. **Analisi**

24. Imposterò la mia analisi nel modo seguente.

25. Le prime due questioni del giudice del rinvio vertono sull'ambito di applicazione del CECE. Con la prima questione si chiede quindi se un regime normativo che richiede un'autorizzazione preventiva per l'uso di hardware e software nelle reti e nei servizi di comunicazione elettronica, come quello introdotto dall'ESS, rientri nell'ambito di applicazione materiale del CECE. Affronterò tale questione nella sezione III.A. La seconda questione mira poi a stabilire se siffatte misure siano comunque escluse dall'ambito di applicazione di tale direttiva in quanto adottate per motivi di sicurezza nazionale. Affronterò tale questione nella sezione III.B. La mia conclusione in merito alle due questioni è che il CECE si applica al caso di specie.

26. Essendo il CECE applicabile, con la terza questione si chiedono orientamenti circa la questione se le misure controverse costituiscano una limitazione alla libertà di fornire reti e servizi di comunicazione elettronica ai sensi dell'articolo 12, paragrafo 1, del CECE. Risponderò in modo affermativo a tale questione nella sezione III.C. Ciò mi porterà alla quarta questione, in cui si chiede di chiarire se tali misure dovessero essere notificate alla Commissione e, in caso affermativo, quali conseguenze risultino dalla loro mancata notifica. Affronterò tale questione nella sezione III.D.

27. Se, come ritengo, le misure nazionali di cui trattasi costituiscono una limitazione della libertà di fornire reti e servizi di comunicazione elettronica, un'altra questione importante che si pone in tale contesto è se, ed eventualmente come, tali misure possano essere giustificate. Tale giustificazione è possibile ai sensi dell'articolo 12, paragrafo 1, del CECE; la suddetta disposizione rinvia a tal riguardo all'articolo 52, paragrafo 1, TFUE. Il giudice del rinvio non chiede tuttavia chiarimenti su come procedere al controllo di proporzionalità ai sensi dell'articolo 12, paragrafo 1, del CECE. Detto giudice pone invece tale questione, sotto forma della quinta questione, in relazione alla libera circolazione delle merci e con la riserva che la Corte ritenga che il CECE non sia applicabile. Poiché proporrò alla Corte di ritenere il CECE applicabile, non sarà necessario rispondere alla quinta questione nella forma in cui è stata sottoposta alla Corte. Tuttavia, il merito di tale questione è rilevante per il giudice del rinvio ai fini della giustificazione di cui all'articolo 12, paragrafo 1, del CECE, in combinato disposto con l'articolo 52, paragrafo 1, TFUE. Di conseguenza, anziché rispondere alla quinta questione nella forma in cui è stata sottoposta alla Corte, proporrò di riformularla come se fosse posta in relazione a queste ultime disposizioni (e non in relazione agli articoli 34 e 36 TFUE). Affronterò la questione in tal modo riformulata nella sezione III.E.

28. Infine, con la sesta questione, il giudice del rinvio chiede assistenza alla Corte per stabilire se le misure di cui trattasi, tenuto conto delle circostanze del caso di specie, costituiscano una privazione di fatto della proprietà della ricorrente, nel qual caso esso ritiene che l'articolo 17, paragrafo 1, della Carta prescriva un'adeguata indennità. Nella sezione III.F suggerirò alla Corte che la misura in questione non costituisce una siffatta privazione, ma rappresenta un'ingerenza nell'uso della proprietà, che può tuttavia essere giustificata e non richiede quindi un'indennità sulla base dell'articolo 17, paragrafo 1, della Carta.

A. Sulla prima questione

29. Con la sua prima questione, il giudice del rinvio chiede, in sostanza, se le disposizioni pertinenti dell'ESS, sulla base delle quali sono state adottate le misure controverse, rientrino nell'ambito di applicazione del CECE.

30. Le posizioni delle parti che hanno presentato osservazioni nella presente causa divergono quanto alla risposta a tale questione. La ricorrente, i governi estone e francese e la Commissione ritengono, in sostanza, che il CECE si applichi alle misure controverse nella presente causa. Il governo estone, sostenuto dalla Commissione, spiega in particolare che l'ESS è stata, di fatto, adottata in attuazione del CECE. Di contro, i governi danese, ceco, italiano, svedese e finlandese ritengono, in sostanza, che il CECE non sia applicabile, atteso che la misura di autorizzazione di cui trattasi è stata adottata al fine di proteggere la sicurezza nazionale dell'Estonia. Da parte sua, il governo spagnolo sostiene che le misure adottate per proteggere la sicurezza nazionale non rientrano nell'ambito di applicazione del CECE, ma che ciò non esonera gli Stati membri dall'obbligo di conformarsi al CECE, che si applica nel caso di specie.

31. Ritengo che il CECE si applichi e che le misure controverse rientrino nell'ambito di applicazione *ratione materiae* di tale direttiva.

32. Il CECE è il principale atto normativo nel settore delle comunicazioni elettroniche. Esso istituisce un quadro normativo armonizzato per garantire un mercato interno delle reti e dei servizi di comunicazione elettronica (17). Per conseguire tale obiettivo, esso mira ad eliminare gli ostacoli alla fornitura di reti e servizi di comunicazione elettronica, vietando le restrizioni imposte dagli Stati membri e adottando norme comuni (18).

33. Tale quadro si applica anche alle reti mobili, di cui trattasi nella presente causa (19).

34. Pertanto, in linea di principio, tutte le norme nazionali relative alla regolamentazione delle reti e dei servizi di comunicazione elettronica rientrano nell'ambito di applicazione del CECE.

35. Uno degli obiettivi del CECE è garantire la sicurezza del mercato interno delle reti e dei servizi di comunicazione elettronica. Quindi, in conformità dell'articolo 1, paragrafo 2, lettera a), tale direttiva mira a «realizzare un mercato interno delle reti e dei servizi di comunicazione elettronica che si traduca in realizzazione e diffusione di reti ad altissima capacità, concorrenza sostenibile, interoperabilità dei servizi di comunicazione elettronica, accessibilità, *sicurezza delle reti e dei servizi* e vantaggi per gli utenti finali» (20).

36. A tal fine, l'articolo 40, paragrafo 1, del CECE impone espressamente agli Stati membri di assicurare che i fornitori di reti o di servizi di comunicazione elettronica pubblici o accessibili al pubblico adottino misure adeguate e proporzionate di natura tecnica e organizzativa per gestire adeguatamente i rischi per la sicurezza delle reti e dei servizi. Tenuto conto delle «attuali conoscenze in materia», tali misure devono assicurare «un livello di sicurezza adeguato al rischio esistente», comprese misure idonee a prevenire e a limitare le conseguenze degli incidenti di sicurezza per gli utenti e per le altre reti e gli altri servizi.

37. Le norme nazionali adottate per conseguire l'obiettivo della «sicurezza delle reti e dei servizi» devono pertanto essere considerate come rientranti nell'ambito di applicazione del CECE.

38. La nozione di «sicurezza delle reti e dei servizi» è definita all'articolo 2, punto 21, del CECE come «la capacità delle reti e dei servizi di comunicazione elettronica di resistere, a un determinato livello di riservatezza, a qualsiasi azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza di tali reti e servizi, dei dati conservati, trasmessi o trattati oppure dei relativi servizi offerti o accessibili tramite tali reti o servizi di comunicazione elettronica».

39. Tale definizione deve essere letta accanto alle definizioni delle nozioni di «reti di comunicazione elettronica» (21) e di «servizio di comunicazione elettronica» (22).

40. La prima di tali nozioni è formulata in modo ampio e comprende, in particolare, le apparecchiature fisiche necessarie alla fornitura di tale rete (e quindi anche l'hardware e il software ivi contenuti) (23). La seconda nozione riguarda la trasmissione di segnali mediante un'infrastruttura fisica, interpretata dalla Corte come estesa anche al software utilizzato, in particolare, per l'accesso a Internet (24).

41. Ne consegue che la nozione di «sicurezza delle reti», quale definita all'articolo 2, punto 21, del CECE, deve essere intesa nel senso che comprende la sicurezza degli elementi tanto *hardware* che *software* di una rete di comunicazione elettronica.

42. Ai fini dell'attuazione dell'articolo 40, paragrafo 1, del CECE, l'articolo 41, paragrafo 1, dello stesso impone agli Stati membri di assicurare che le competenti autorità abbiano la facoltà di impartire istruzioni vincolanti, compreso in materia di misure necessarie per evitare che si verifichi un incidente di sicurezza nel caso in cui sia stata individuata una «minaccia significativa».

43. Non sono previste ulteriori disposizioni per quanto riguarda le norme che gli Stati membri devono adottare a tal riguardo. Pertanto, il diritto dell'Unione lascia agli Stati membri la decisione su come attuare tali requisiti al fine di garantire la sicurezza delle loro reti e dei loro servizi.

44. Nel caso di specie, dalla decisione di rinvio, dalle osservazioni della ricorrente nonché dalle osservazioni del governo estone e del KJN, confermate in udienza, risulta che la normativa di cui trattasi mira ad attuare il CECE, in particolare l'articolo 40, paragrafo 1, e l'articolo 41, paragrafo 1, nel diritto estone.

45. Non vi è motivo per cui una procedura di autorizzazione *ex ante* per l'uso di hardware e software per la fornitura di reti e servizi di comunicazione elettronica, come quella richiesta dall'ESS, non debba essere considerata una delle possibilità di configurare l'attuazione dell'articolo 40, paragrafo 1, e dell'articolo 41, paragrafo 1, del CECE.

46. Ciò non è nemmeno contestato nel caso di specie.

47. Alla luce di quanto sopra, propongo alla Corte di rispondere affermativamente alla prima questione sollevata dal giudice del rinvio, vale a dire che il CECE deve essere interpretato nel senso che esso è applicabile a un insieme di disposizioni legislative e regolamentari nazionali che, al fine di garantire la sicurezza della rete nazionale di comunicazioni elettroniche e dei relativi servizi, impongono a un operatore che intenda fornire tale rete e tali servizi di ottenere un'autorizzazione d'uso di hardware e software nella propria rete di comunicazioni.

B. Sulla seconda questione

48. Con la sua seconda questione, che è subordinata a una risposta affermativa alla prima questione, il giudice del rinvio chiede, in sostanza, se l'effetto dell'articolo 4, paragrafo 2, TUE e dell'articolo 1, paragrafo 3, lettera c), del CECE sia tale da far rientrare le misure di autorizzazione di cui trattasi nella competenza esclusiva degli Stati membri ai quali il CECE non si applica, dal momento che tali misure sono state adottate al fine di garantire la sicurezza nazionale.

49. Non occorre che mi dilunghi sulla questione.

50. L'ultima frase dell'articolo 4, paragrafo 2, TUE stabilisce che la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro. La stessa idea si riflette nell'articolo 1, paragrafo 3, lettera c), del CECE, che prevede che tale direttiva si applica fatte salve le misure adottate dagli Stati membri per fini di ordine pubblico, pubblica sicurezza e difesa.

51. Pertanto, nonostante le differenze terminologiche tra le due disposizioni (25), condivido il parere della Commissione e del governo francese secondo cui l'articolo 1, paragrafo 3, lettera c), del CECE costituisce, in sostanza, un'espressione dell'articolo 4, paragrafo 2, TUE.

52. La questione è se tali due disposizioni debbano essere interpretate nel senso che le misure adottate per motivi di sicurezza nazionale devono essere escluse dall'ambito di applicazione del CECE.

53. La ricorrente, i governi estone, spagnolo e francese nonché la Commissione ritengono che, se è vero che gli Stati membri possono decidere autonomamente misure volte a tutelare la loro sicurezza nazionale, ciò non li esime dal conformarsi al CECE. L'effetto dell'articolo 4, paragrafo 2, TUE e dell'articolo 1, paragrafo 3, lettera c), del CECE non è quindi tale da escludere dall'ambito di applicazione del diritto dell'Unione la misura di autorizzazione di cui trattasi. Aderendo alla tesi contraria, i governi danese, ceco, italiano, svedese e finlandese sottolineano che, tenuto conto del fatto che le misure in questione sono state adottate al fine di tutelare la sicurezza nazionale dell'Estonia, l'effetto dell'articolo 4, paragrafo 2, TUE e dell'articolo 1, paragrafo 3, lettera c), del CECE è tale da escludere l'applicazione del diritto dell'Unione.

54. A mio avviso, la giurisprudenza della Corte spiega già che l'articolo 4, paragrafo 2, TUE non esclude le misure di sicurezza nazionale dall'ambito di applicazione del diritto dell'Unione (26).

55. Tale disposizione conferma piuttosto che l'Unione europea non è competente a decidere che cosa è necessario per proteggere la sicurezza degli Stati membri e come farlo. Ciò nonostante, sebbene, ai sensi dell'articolo 4, paragrafo 2, TUE, la sicurezza nazionale resti di esclusiva competenza di ciascuno Stato membro, «la mera circostanza che una misura nazionale sia stata adottata ai fini della tutela della sicurezza nazionale non può comportare l'inapplicabilità del diritto dell'Unione e dispensare gli Stati membri dal necessario rispetto di tale diritto» (27).

56. Pertanto, anche se l'Estonia ha adottato la normativa controversa al fine di proteggere la propria sicurezza nazionale, ciò non esclude tale normativa e le misure adottate sulla base di essa dall'ambito di applicazione del CECE.

57. In altri termini, qualora le misure adottate per tutelare la sicurezza nazionale siano contrarie alle norme dell'Unione, l'interesse pubblico alla tutela della sicurezza nazionale può essere invocato per giustificare tale conflitto; tuttavia, affinché sia dimostrata la loro legittimità, tali misure devono soddisfare il criterio di proporzionalità. Tornerò su questo punto nell'ambito della risposta alla quinta questione.

58. Nella presente causa, come ho già spiegato, il governo estone ritiene per l'appunto che la normativa di cui trattasi tuteli gli interessi della sicurezza nazionale, ma che essa sia, al contempo, adottata in esecuzione del CECE (28). Infatti, per giustificare le sue decisioni amministrative nazionali che considerano gli hardware e i software di cui trattasi come fonte di «rischio elevato» per la sicurezza delle sue infrastrutture di telecomunicazione, il governo estone si basa su taluni strumenti di *soft law* dell'Unione elaborati dalla Commissione europea (29) e da un gruppo di cooperazione delle agenzie nazionali di sicurezza (30).

59. Vi è pertanto una convergenza tra le preoccupazioni dell'Estonia in materia di sicurezza *nazionale* e i requisiti di sicurezza stabiliti a *livello dell'Unione*.

60. Detto elemento distingue la presente causa dalla sentenza *Ministrstvo za obrambo* (31). Nell'ambito di tale causa, la Corte ha ritenuto che talune categorie di attività militari non rientrassero nell'ambito di applicazione della direttiva 2003/88/CE, concernente taluni aspetti dell'organizzazione dell'orario di lavoro (32), «qualora tali attività [fossero] talmente specifiche da ostare in modo imperativo e permanente al rispetto dei requisiti imposti da tale direttiva» (33).

61. Sulla base di quanto precede, propongo alla Corte di rispondere in senso negativo alla seconda questione e di dichiarare che l'articolo 4, paragrafo 2, TUE e l'articolo 1, paragrafo 3, lettera c), del CECE devono essere interpretati nel senso che una misura che prescrive l'autorizzazione di hardware e software per la fornitura di una rete o di un servizio di comunicazione elettronica pubblici o accessibili al pubblico non è esclusa dall'ambito di applicazione del CECE, anche se tale misura è stata adottata al fine di tutelare gli interessi della sicurezza nazionale.

C. Sulla terza questione

62. Dalle mie risposte alle prime due questioni discende che l'ESS e le decisioni impugnate, adottate sulla base dell'ESS, rientrano nell'ambito di applicazione del CECE. Ciò mi conduce alla terza questione pregiudiziale.

63. Con la sua terza questione, il giudice del rinvio chiede, in sostanza, se una misura nazionale che prescrive un'autorizzazione preventiva per l'uso di hardware e software costituisca una limitazione della libertà di fornire reti e servizi di comunicazione elettronica ai sensi dell'articolo 12, paragrafo 1, del CECE.

64. La ricorrente ritiene che a tale questione occorra rispondere in senso affermativo. Essa sostiene che l'articolo 12, paragrafo 1, del CECE impone agli Stati membri di garantire la libera prestazione dei servizi di comunicazione elettronica, che risulta limitata dalla procedura di autorizzazione nell'ESS. I governi estone, spagnolo, francese e italiano nonché la Commissione non condividono tale posizione. Essi sostengono, in sostanza, che la procedura di autorizzazione prevista dall'ESS costituisce una condizione preliminare alla libertà di fornire servizi di comunicazione elettronica, e non una restrizione, atteso che la libera prestazione dei servizi di comunicazione elettronica, ai sensi dell'articolo 12, paragrafo 1, del CECE, è garantita «fatte salve le condizioni stabilite nella presente direttiva». Secondo tale tesi, poiché la sicurezza delle reti e dei servizi di comunicazione elettronica costituisce una di tali condizioni, gli Stati membri possono legittimamente prevedere una procedura di autorizzazione come quella di cui trattasi nel procedimento principale (34).

65. Da tali prese di posizione scaturisce che la Corte dispone di due opzioni quanto alla qualificazione della misura di autorizzazione di cui trattasi ai sensi dell'articolo 12, paragrafo 1, del CECE: i) come *condizione* per la fornitura di reti e servizi di comunicazione elettronica o ii) come *restrizione* alla fornitura di tali reti e servizi.

66. Ritengo che un siffatto requisito costituisca una restrizione alla fornitura di tali reti e servizi, ai sensi dell'articolo 12, paragrafo 1, del CECE. Tuttavia, ritengo che tale restrizione sia giustificata.

67. A tale riguardo, è opportuno ricordare le prime due frasi dell'articolo 12, paragrafo 1, del CECE:

«Gli Stati membri *garantiscono* la libertà di fornire reti e servizi di comunicazione elettronica, fatte salve le condizioni stabilite nella presente direttiva. A tal fine, gli Stati membri *non impediscono* alle imprese di fornire reti o servizi di comunicazione elettronica, salvo quando ciò si renda necessario per i motivi di cui all'articolo 52, paragrafo 1, TFUE» (35).

68. Pertanto, in linea di principio, la situazione normale derivante da tale disposizione è che, fatte salve determinate condizioni, gli Stati membri devono *consentire* alle imprese di fornire reti e servizi di comunicazione elettronica.

69. Inoltre, gli Stati membri non possono *impedire* a tali imprese di esercitare la suddetta libertà mediante restrizioni che non siano imposte direttamente dallo stesso CECE quali condizioni per la fornitura di tali reti e servizi di comunicazione elettronica.

70. Contemporaneamente all'imposizione dell'*integrazione negativa* (vale a dire il divieto delle misure degli Stati membri che creano ostacoli alla libertà di fornire reti e servizi di comunicazione elettronica) (36), l'articolo 12, paragrafo 1, del CECE riconosce anche la necessità di un'*integrazione positiva* (vale a dire l'armonizzazione della necessità di garantire la sicurezza come condizione per la fornitura di reti e di servizi di comunicazione elettronica).

71. Tuttavia, sebbene venga richiesto che le reti e i servizi siano sicuri, non si riscontra al livello dell'Unione un'integrazione positiva per quanto riguarda la sicurezza di tali reti e servizi.

72. Il CECE non prevede quali misure garantiscano tale sicurezza. Esso lascia la scelta agli Stati membri imponendo a essi, mediante l'articolo 40, paragrafo 1, e l'articolo 41, paragrafo 1, dello stesso, di operare tali scelte.

73. In altri termini, anche se, ai sensi del CECE, la sicurezza delle reti e dei servizi costituisce una condizione per la fornitura di tali reti e servizi, la previa autorizzazione d'uso di hardware e software nell'ambito di tale fornitura non lo è.

74. Il contrario, vale a dire se qualsiasi misura che uno Stato membro sceglie di adottare per garantire la sicurezza delle reti e dei servizi fosse automaticamente qualificata come condizione per il corretto funzionamento del mercato interno delle reti e dei servizi di comunicazione elettronica, significherebbe che gli Stati membri potrebbero facilmente creare ostacoli alla libera circolazione (37).

75. La suddetta esclusione automatica dal controllo giurisdizionale di proporzionalità delle misure scelte dagli Stati membri sarebbe in contrasto con l'obiettivo dell'articolo 12, paragrafo 1, del CECE di prevenire gli ostacoli alla libera prestazione di reti e di servizi di comunicazione elettronica.

76. Propongo quindi un'interpretazione secondo la quale una specifica misura nazionale adottata al fine di garantire la sicurezza delle reti e dei servizi di uno Stato membro può essere qualificata come restrizione alla libera fornitura di tali reti e servizi, vietata dall'articolo 12, paragrafo 1, del CECE, sebbene gli Stati membri siano tenuti, in forza di tale direttiva, a garantire la sicurezza delle loro reti.

77. Qualsiasi obbligo di autorizzazione preventiva per accedere al mercato interno è, in linea di principio, considerato un ostacolo alla libera circolazione, che si tratti di merci (38), servizi (39), capitali (40) o della libertà di stabilimento (41). Un siffatto obbligo rende sempre meno interessante la libertà e più difficile l'accesso ai mercati interessati.

78. A tal riguardo, è evidente che una procedura di autorizzazione preventiva, come quella di cui trattasi nel caso di specie, che consente alle autorità competenti di vietare l'uso di determinati hardware e software a causa del loro carattere «ad alto rischio», costituisce una misura che, in linea di principio, rappresenta un ostacolo alla libera circolazione delle reti e dei servizi di comunicazione elettronica, in quanto è idonea a rendere meno attraente o più difficile l'accesso a tale servizio e il suo funzionamento.

79. Pertanto, tale misura è, in linea di principio, vietata dall'articolo 12, paragrafo 1, del CECE.

80. La normativa estone di cui trattasi è quindi idonea a limitare la libera prestazione delle reti e dei servizi di comunicazione elettronica, in violazione dell'articolo 12, paragrafo 1, prima frase, del CECE.

81. Ciò premesso, in forza dell'articolo 12, paragrafo 1, del CECE, una siffatta misura può essere giustificata da uno dei motivi elencati all'articolo 52, paragrafo 1, TFUE.

82. L'analisi di proporzionalità che ne deriva, che comprende considerazioni di sicurezza nazionale, rientra nella competenza del giudice del rinvio. Detto giudice non ha chiesto orientamenti su tale particolare

aspetto dell'articolo 12, paragrafo 1, del CECE. Ciò premesso, con riferimento alla risposta che propongo alla quinta questione, fornisco al giudice del rinvio un orientamento che può essere utile anche a tal riguardo.

83. Sulla base di quanto precede, suggerisco alla Corte di rispondere alla terza questione in senso affermativo: l'articolo 12, paragrafo 1, del CECE deve essere interpretato nel senso che un insieme di disposizioni legislative e regolamentari nazionali che prescrive l'autorizzazione di un'autorità amministrativa per l'uso di hardware e software nella fornitura di reti e servizi di comunicazione elettronica costituisce una limitazione della libertà di fornire reti e servizi, ai sensi di detta disposizione. Una simile limitazione può essere giustificata dai motivi previsti all'articolo 52, paragrafo 1, TFUE.

D. Sulla quarta questione

84. L'articolo 12, paragrafo 1, terza frase, del CECE impone agli Stati membri di motivare debitamente qualsiasi limitazione alla libertà di fornire reti e servizi di comunicazione elettronica e di comunicare alla Commissione una siffatta limitazione.

85. Alla luce di tale disposizione, il giudice del rinvio chiede, con la sua quarta questione, quali conseguenze derivino dalla mancata comunicazione di una limitazione al diritto di cui all'articolo 12, paragrafo 1, del CECE, quale, nel caso di specie, un insieme di disposizioni legislative e regolamentari che richiede una preventiva autorizzazione d'uso di hardware e software nelle reti di comunicazione elettronica. In particolare, detto giudice chiede se la mancata comunicazione in parola renda inapplicabile tale misura.

86. Secondo la ricorrente, la normativa di cui trattasi non è stata comunicata alla Commissione. Per tale ragione, non può essere applicata nei suoi confronti la procedura di autorizzazione prevista dall'ESS. I governi estone, spagnolo, francese e italiano nonché la Commissione, sostenuti in udienza anche dal TTJA nonché dai governi tedesco e finlandese, sostengono che non era necessaria alcuna comunicazione, in quanto, a loro avviso, l'obbligo di autorizzazione derivante dall'ESS non costituisce una restrizione, bensì una condizione imposta dal CECE per la fornitura di reti e servizi di comunicazione elettronica.

87. Contrariamente a tali posizioni, come ho già spiegato nell'ambito della terza questione, a mio avviso una misura di autorizzazione preventiva, come quella introdotta in Estonia dall'ESS, costituisce una limitazione della libertà di fornire reti e servizi di comunicazione elettronica. Pertanto, a mio parere, una misura di tale tipo avrebbe dovuto essere comunicata alla Commissione.

88. Tuttavia, vorrei osservare che dal fascicolo non risulta chiaramente se tale misura fosse stata effettivamente comunicata. Secondo il governo estone, una bozza dell'ESS, comprendente il quadro autorizzativo, è stata comunicata alla Commissione nel 2020 (42), prima della sua entrata in vigore nel 2022. La ricorrente, tuttavia, contesta l'esistenza di una siffatta comunicazione. Spetta al giudice del rinvio verificare se sia effettivamente avvenuto ciò.

89. Ciò detto, anche se il governo estone non avesse comunicato alla Commissione l'obbligo di legge dell'autorizzazione preventiva, ritengo che tale omissione non comporti l'inapplicabilità di tale parte dell'ESS nei confronti della ricorrente, vale a dire che l'effetto della mancata comunicazione non è lo stesso che si verificherebbe in caso di mancata comunicazione dei requisiti tecnici previsti dalla direttiva TRIS.

90. In primo luogo, la direttiva TRIS esclude espressamente la sua applicazione nel settore delle reti e dei servizi di comunicazione elettronica. Il suo articolo 1, paragrafo 3, stabilisce che essa «non si applica a regole concernenti questioni che costituiscono oggetto di una normativa dell'Unione in materia di servizi di telecomunicazione, di cui [alla direttiva che ha preceduto il CECE]».

91. Ai fini delle regole e delle norme tecniche relative alle reti e ai servizi di comunicazione elettronica, il CECE rappresenta pertanto una *lex specialis* rispetto alla direttiva TRIS.

92. In secondo luogo, come spiegato dalla Commissione, non si può stabilire alcuna analogia tra la mancata comunicazione ai sensi dell'articolo 12, paragrafo 1, del CECE, da un lato, e il mancato rispetto della procedura di comunicazione istituita dalla direttiva TRIS e dalla giurisprudenza pertinente, dall'altro, secondo la quale la mancata comunicazione di una norma tecnica comporta la sua inapplicabilità nei confronti dei singoli (43).

93. Ciò perché, contrariamente alla direttiva TRIS, l'articolo 12, paragrafo 1, del CECE non subordina l'applicabilità delle condizioni relative alla fornitura di reti e di servizi di comunicazione elettronica all'approvazione della Commissione o alla scadenza di un termine minimo.

94. Pertanto, la mancata comunicazione di una limitazione alla libertà di fornire reti e servizi di comunicazione elettronica ai sensi dell'articolo 12, paragrafo 1, del CECE non comporta l'impossibilità di applicare alla ricorrente la procedura di autorizzazione prevista dall'ESS.

95. Per le ragioni che precedono, propongo alla Corte di rispondere alla quarta questione dichiarando che la mancata comunicazione alla Commissione di una limitazione della libertà di fornire reti di comunicazione elettronica, ai sensi dell'articolo 12, paragrafo 1, del CECE, non comporta l'inapplicabilità della normativa nazionale non comunicata.

E. Sulla quinta questione

96. La quinta questione, così come sollevata, verte su misure nazionali che limitano la libera circolazione delle merci, quale prevista all'articolo 34 TFUE, ma che possono essere giustificate sulla base dell'articolo 36 TFUE. Tale questione è stata sottoposta alla Corte a condizione che essa ritenga che il CECE non sia applicabile.

97. Tuttavia, come ho spiegato, ritengo che il CECE sia applicabile al caso di specie. Pertanto, in linea di principio, non occorre che la Corte risponda alla quinta questione.

98. Ciò premesso, in sostanza, la risposta a tale questione come sollevata sarebbe utile al giudice del rinvio per decidere se le misure controverse introdotte sulla base dell'ESS possano essere giustificate ai sensi dell'articolo 12, paragrafo 1, del CECE, in forza del quale esse costituiscono una limitazione.

99. Poiché la Corte ha la possibilità di riformulare una questione che le è stata sottoposta nel modo che ritiene utile per la decisione nel procedimento dinanzi al giudice del rinvio, propongo che la Corte proceda in tal senso nel caso di specie (44).

100. Come riformulata, con la quinta questione si chiederebbe pertanto se sia compatibile con l'articolo 12, paragrafo 1, del CECE e con il principio di proporzionalità il fatto che, al fine di garantire la sicurezza nazionale, le disposizioni legislative e regolamentari nazionali impongano a un'impresa di comunicazione di ottenere un'autorizzazione d'uso di hardware e software nella propria rete di comunicazione, e non obblighino invece l'autorità amministrativa, in sede di valutazione della minaccia derivante da hardware e software ad alto rischio: (a) ad esaminare se i rischi associati al produttore si riflettano sugli specifici hardware e software; (b) a valutare la funzionalità, l'ubicazione e la rilevanza degli specifici hardware e software nell'ambito della fornitura di un servizio di comunicazione, e (c) a verificare se i problemi associati allo Stato di stabilimento del produttore si riverberino su quest'ultimo.

101. A tal riguardo, è importante sottolineare che il giudice del rinvio non chiede una risposta in merito alla proporzionalità delle decisioni impugnate e adottate sulla base dell'ESS. Tale giudice chiede piuttosto un orientamento in merito alla giustificabilità della procedura di autorizzazione disciplinata dall'ESS, su cui si basano le decisioni impugnate, qualora essa non imponga alle autorità competenti l'obbligo di valutare anzitutto se il rischio per la sicurezza nazionale sia reale, prima di respingere la domanda di autorizzazione

per tali motivi. Solo se l'ESS è ritenuta valida da tale punto di vista, si pone la questione della proporzionalità delle modalità di attuazione.

102. Una misura che costituisce una limitazione della libertà di fornire reti e servizi di comunicazione elettronica, ai sensi dell'articolo 12, paragrafo 1, del CECE, può essere giustificata per i motivi di cui all'articolo 52, paragrafo 1, TFUE, vale a dire ordine pubblico, pubblica sicurezza e sanità pubblica.

103. Nel caso di specie, il governo estone giustifica la limitazione introdotta dall'ESS sulla base della sicurezza nazionale (nel senso della sicurezza delle sue infrastrutture di telecomunicazioni) e del fatto che tali misure attuano il CECE, in particolare l'articolo 40, paragrafo 1, e l'articolo 41, paragrafo 1.

104. È pacifico che la sicurezza delle reti di comunicazione è di fondamentale importanza nelle odierne società democratiche: un'infrastruttura di telecomunicazioni sicura e affidabile non solo è necessaria per l'efficace esercizio di una serie di valori e diritti fondamentali dell'Unione, tra cui il valore della democrazia e la libertà di espressione, ma garantisce anche la stabilità sociale, atteso che l'influenza sull'infrastruttura di telecomunicazioni di uno Stato membro, o le turbative della stessa, possono incidere su altri settori dell'economia e, più in generale, sulla vita quotidiana dei cittadini dell'Unione (45).

105. Osservo altresì che la Corte ha già riconosciuto che la sicurezza dell'infrastruttura di telecomunicazioni di uno Stato membro può costituire un elemento della pubblica sicurezza di uno Stato membro (46).

106. Inoltre, il CECE persegue l'obiettivo di garantire la sicurezza delle reti e dei servizi di comunicazione elettronica e, a tal fine, in forza dell'articolo 40, paragrafo 1, e dell'articolo 41, paragrafo 1, impone agli Stati membri di garantire la sicurezza delle loro reti e dei loro servizi di comunicazione elettronica (47).

107. Tuttavia, anche se la sicurezza della rete di comunicazione elettronica di uno Stato membro e dei relativi servizi è riconosciuta come un interesse fondamentale della società sia a livello degli Stati membri sia a livello dell'Unione, e può quindi essere invocata come giustificazione per limitare la libertà di fornire tali reti e servizi, la suddetta limitazione può essere imposta solo se il rischio relativo a tale interesse è reale, attuale e sufficientemente grave nel caso specifico (48).

108. A tal riguardo, uno Stato membro non può giustificare una siffatta restrizione invocando unicamente motivi di sicurezza nazionale (49).

109. Al contrario, la normativa che consente tale restrizione, nella fattispecie l'ESS, deve obbligare le autorità competenti, nella fattispecie il TTJA e il KJN, a valutare se le particolari apparecchiature di cui trattasi rappresentino effettivamente un tale rischio per la sicurezza della rete nazionale di telecomunicazioni.

110. Sebbene tale valutazione possa essere diversa per quanto riguarda rischi proveniente da paesi terzi o dai loro fornitori (50), essa non può basarsi su un sospetto generico (51); al contrario, essa deve ricomprendere una valutazione concreta dell'uso cui tali apparecchiature sono destinate e dei rischi ad esso associati. Tale analisi può riguardare, ad esempio, rischi connessi al tipo di apparecchiatura di cui trattasi, al produttore di quest'ultima o ancora allo Stato in cui tale produttore è stabilito (52).

111. Alla luce di ciò, occorre rispondere alla quinta questione del giudice del rinvio dichiarando che l'articolo 12, paragrafo 1, del CECE esige che disposizioni legislative e regolamentari nazionali, che impongono di ottenere un'autorizzazione preventiva d'uso di hardware e software al fine di tutelare la sicurezza delle reti e dei servizi di comunicazione elettronica, obblighino gli organismi abilitati a decidere in merito alla concessione di una siffatta autorizzazione a valutare se l'hardware e il software di cui trattasi, di cui si chiede l'uso, presentino un rischio reale per la sicurezza della rete, il che può includere la presa in considerazione dell'uso cui tali apparecchiature sono destinate, nonché delle questioni se i rischi associati allo Stato di

stabilimento del produttore si riflettano su quest'ultimo e se i rischi associati al produttore si riflettano sugli specifici hardware e software.

112. A quanto mi risulta, tema che spetta al giudice del rinvio verificare, l'ESS stabilisce criteri precisi sulla base dei quali le autorità nazionali competenti possono concludere che sussiste un rischio per la sicurezza nazionale. A tal fine, sembra che si tenga conto, tra l'altro, dell'esistenza di una minaccia relativa al produttore e al paese terzo in cui tale produttore è stabilito (53).

113. In sede di controllo delle decisioni impugnate, il giudice nazionale dovrà valutare se tali criteri siano stati effettivamente presi in considerazione durante la valutazione dei rischi nella situazione particolare del caso di specie, con conseguente limitazione temporale del permesso d'uso.

114. Posto che ciò richiede una conoscenza approfondita degli aspetti tecnici, politici e di sicurezza connessi a una situazione particolare, la valutazione dell'esistenza di un rischio rispetto a un determinato produttore, alle sue apparecchiature o al loro utilizzo non può essere effettuata dai giudici dell'Unione. Tuttavia, quando un giudice nazionale è chiamato a riesaminare le misure che vietano l'uso di determinati hardware e software per motivi di sicurezza nazionale, le autorità competenti devono essere in grado di fornire spiegazioni ragionevoli dei motivi per cui è stato individuato tale rischio (54); se del caso, ciò può richiedere l'utilizzo di tecniche giudiziarie diverse (55).

115. Qualora, come nel caso di specie, vi sia una convergenza tra gli interessi in materia di sicurezza di cui trattasi a livello dell'Unione e a livello nazionale, un giudice nazionale può anche prendere in considerazione – nell'ambito del controllo giurisdizionale della misura di cui trattasi – le valutazioni dei rischi effettuate dalle istituzioni e dagli organi dell'Unione nonché da organi nazionali.

116. In tal senso, diversi documenti invocati dal governo estone potrebbero essere pertinenti per la valutazione del giudice del rinvio: tale governo fa riferimento, in particolare, alla raccomandazione della Commissione del 2019 sulla cibersicurezza, alla valutazione coordinata dei rischi e al pacchetto di strumenti sul 5G (56) del gruppo di cooperazione NIS (57), nonché alla comunicazione della Commissione sull'attuazione del pacchetto di strumenti sul 5G.

117. Sebbene tali documenti costituiscano elementi di *soft law* non vincolanti per gli Stati membri, essi prevedono una valutazione coordinata dei rischi da parte delle autorità competenti a livello nazionale e dell'Unione, sulla base della quale la Commissione ha individuato, tra l'altro, le apparecchiature fabbricate dal produttore degli hardware e software di cui trattasi come aventi «rischi materialmente più elevati di altri fornitori di 5G» e ha stabilito che, in virtù di «tali rischi elevati, (…) la Commissione ritiene che le decisioni adottate dagli Stati membri volte a limitare l'accesso di Huawei (…) o a escluderl[a] siano giustificate e conformi al pacchetto di strumenti sul 5G» (58).

118. Secondo la comunicazione sull'attuazione del pacchetto di strumenti sul 5G, tale conclusione si basa tra l'altro, sul fatto che esiste un «legame tra [tale] fornitore e il governo di un determinato paese terzo, la legislazione del paese terzo e le caratteristiche della proprietà societaria del fornitore» (59).

119. Il governo estone spiega che le sue autorità competenti hanno tenuto conto di tale valutazione e che, in forza di tale identificazione comune dei rischi sia a livello dell'Unione sia a livello degli Stati membri, esse hanno ritenuto necessario limitare l'esposizione alle apparecchiature provenienti, in particolare, dalla Huawei, fornitore degli hardware e software di cui trattasi, nella fornitura di reti e servizi di comunicazione elettronica.

120. Di conseguenza, mi sembra ragionevole concludere che l'ESS e le decisioni impugnate, adottate sulla base di esso, pur costituendo una restrizione alla libertà di fornire reti e servizi di comunicazione elettronica,

perseguono un obiettivo legittimo: la prevenzione di un rischio reale per la sicurezza delle reti. Tale valutazione spetta tuttavia al giudice nazionale.

F. Sulla sesta questione

121. Dal fascicolo nazionale risulta che gli hardware e software di cui trattasi erano utilizzati dalla ricorrente per la funzionalità 2G-4G per la fornitura di reti e servizi di comunicazione elettronica prima delle decisioni impugnate. Dalle spiegazioni della ricorrente risulta altresì che essa aveva acquistato apparecchiature per la funzionalità 5G al fine di includerle nel suo perimetro di rete prima dell'introduzione dell'obbligo di autorizzazione nell'ESS. Infine, dalla decisione del giudice del rinvio e dalle spiegazioni delle parti risulta che le decisioni impugnate autorizzavano l'utilizzo degli hardware e software di cui trattasi per un periodo più breve rispetto alla durata di vita utile di tali apparecchiature.

122. A tal riguardo, con la sesta questione il giudice del rinvio chiede se, tenuto conto di tali circostanze, le decisioni impugnate comportino una privazione della proprietà ai sensi dell'articolo 17, paragrafo 1, seconda frase, della Carta, nel qual caso la ricorrente potrebbe avere diritto a un'indennità adeguata.

123. La ricorrente ritiene che tale sia il caso. Essa sostiene che il regime di autorizzazione di cui trattasi comporta una privazione ingiustificata della proprietà. Essa ritiene altresì che una modifica improvvisa del regime legislativo che disciplina l'utilizzo degli hardware e software di cui trattasi, la quale introduce un requisito di autorizzazione d'uso e comporta il divieto di utilizzo di hardware e software che la ricorrente ha legalmente acquistato presso un determinato produttore, sia esclusa dall'articolo 17, paragrafo 1, della Carta, a meno che non sia prevista un'indennità giusta e adeguata.

124. Secondo la Commissione e i governi estone, spagnolo, tedesco, francese, italiano, svedese e finlandese, il contesto che accompagna la misura di autorizzazione di cui trattasi costituisce un tipo di regolamentazione dell'uso dei beni ai sensi dell'articolo 17, paragrafo 1, terza frase, della Carta. Pertanto, le decisioni impugnate non hanno comportato una privazione, di fatto o di diritto, della proprietà della ricorrente degli hardware e software di cui trattasi. Tali parti ritengono inoltre che detta regolamentazione sulla proprietà, alla luce delle preoccupazioni di sicurezza nazionale e pubblica dell'Estonia, costituisca una restrizione proporzionata di tale diritto, atteso che le autorità estoni hanno previsto un periodo transitorio sufficientemente lungo.

125. Conformemente all'articolo 17, paragrafo 1, della Carta «[o]gni persona ha il diritto di godere della proprietà dei beni che ha acquisito legalmente, di usarli, di disporne e di lasciarli in eredità. Nessuna persona può essere privata della proprietà se non per causa di pubblico interesse, nei casi e nei modi previsti dalla legge e contro il pagamento in tempo utile di una giusta indennità per la perdita della stessa. L'uso dei beni può essere regolato dalla legge nei limiti imposti dall'interesse generale».

126. La Corte ha statuito che tale disposizione contiene tre norme distinte. Ha spiegato che «[l]a prima, che si esprime nella prima frase di tale disposizione e riveste carattere generale, concretizza il principio del rispetto della proprietà. La seconda, contenuta nella seconda frase di detta disposizione, riguarda la privazione della proprietà e la subordina a talune condizioni. Quanto alla terza, contenuta nella terza frase della medesima disposizione, essa riconosce agli Stati membri il potere di regolamentare l'uso dei beni nei limiti imposti dall'interesse generale. Tali norme non sono tuttavia prive di rapporto tra loro. Infatti, la seconda e la terza norma riguardano esempi particolari di violazione del diritto di proprietà e devono essere interpretate alla luce del principio sancito dalla prima di esse» (60).

127. Dalla giurisprudenza della Corte risulta inoltre che la tutela conferita dall'articolo 17, paragrafo 1, della Carta è ampia e comprende, oltre ai beni aventi un valore economico, gli interessi connessi allo sfruttamento di una licenza o di un'autorizzazione d'uso (61).

128. Nel procedimento principale, le decisioni impugnate riguardano una richiesta di autorizzazione all'uso di taluni hardware e software nella fornitura di reti e servizi di comunicazione elettronica. Tale richiesta è stata accolta solo parzialmente e limitatamente alla durata massima prevista dall'ESS: vale a dire, fino al 31 dicembre 2029 per la funzionalità 2G-4G e fino al 31 dicembre 2025 per la funzionalità 5G.

129. Di conseguenza, dal momento che non sussisteva alcuna ingerenza sul contenuto essenziale di tale proprietà, la ricorrente non ne è stata privata (62). Invece, le decisioni impugnate rappresentano una limitazione dell'uso della proprietà della ricorrente ai sensi dell'articolo 17, paragrafo 1, terza frase, della Carta (63).

130. In tal caso, il ricorrente non ha, in linea di principio, diritto all'indennità.

131. Ciò premesso, la limitazione dell'uso dei beni è possibile solo nella misura in cui sia necessaria per l'interesse generale. Ai fini della presente causa, tale valutazione sarà simile a quella richiesta per giustificare un'ingerenza nella libertà di fornire reti e servizi di comunicazione elettronica ai sensi dell'articolo 12, paragrafo 1, del CECE.

132. Tuttavia, il giudice del rinvio non ha chiesto indicazioni su come procedere a un siffatto esame di proporzionalità.

133. Osservo nondimeno che uno degli aspetti che il giudice del rinvio dovrebbe prendere in considerazione nel caso di specie è se la durata del periodo durante il quale la ricorrente è stata autorizzata a continuare a utilizzare gli hardware e software di cui trattasi, nel contesto della durata del periodo che consente alla ricorrente di prepararsi a tale modifica normativa, fosse sufficiente.

134. Ciò in quanto la misura di autorizzazione di cui trattasi, unitamente a rigorosi periodi massimi di utilizzo, incide in modo considerevole sugli investimenti effettuati prima dell'introduzione di tali modifiche legislative (64).

135. Pertanto, il giudice del rinvio deve valutare se l'intero periodo durante il quale la ricorrente avrebbe potuto prepararsi ad adeguarsi alla nuova situazione legislativa, dal momento in cui sono state proposte le modifiche pertinenti dell'ESS fino alla fine del periodo massimo di utilizzo degli hardware e software di cui trattasi, fosse di durata sufficiente. Se ritiene che tale non sia il caso, andrebbe preso in considerazione un sistema di ragionevole ristoro del danno subìto (65).

136. Infine, in sede di valutazione della proporzionalità delle decisioni impugnate, il giudice del rinvio dovrebbe tener conto della gravità dell'ingerenza nel diritto fondamentale di cui trattasi e dell'importanza dell'obiettivo perseguito (66) nonché di altri interessi, quali l'interesse dei destinatari di reti e di servizi di comunicazione elettronica alla sicurezza di tali reti e servizi, nonché il rischio di mercato che un concorrente prudente e avveduto, attivo sullo stesso mercato, avrebbe assunto per quanto riguarda gli hardware e software di cui trattasi (67).

137. Ove il giudice del rinvio ritenga che l'onere gravante sulla ricorrente sia sproporzionato, anche se necessario, potrebbe essere opportuno, come ho spiegato, fare ricorso a una giusta indennità.

138. Sulla base delle considerazioni che precedono, propongo alla Corte di rispondere alla sesta questione dichiarando che una limitazione dell'uso di hardware o software preesistenti, in una rete di comunicazione elettronica, all'introduzione dell'obbligo di autorizzazione d'uso, in forza del quale l'uso è concesso per un periodo inferiore alla vita utile di tale hardware o software, non costituisce una privazione della proprietà ai sensi dell'articolo 17, paragrafo 1, seconda frase, della Carta.

IV. **Conclusione**

139. Propongo alla Corte di rispondere alle questioni sottoposte dal Tallinna Halduskohus (Tribunale amministrativo di Tallinn, Estonia) come segue:

1) La direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche,

deve essere interpretata nel senso che essa è applicabile a un insieme di disposizioni legislative e regolamentari nazionali che, al fine di garantire la sicurezza della rete nazionale di comunicazioni elettroniche e dei relativi servizi, impongono a un operatore che intenda fornire tale rete e tali servizi di ottenere un'autorizzazione d'uso di hardware e software nella propria rete di comunicazioni.

2) L'articolo 4, paragrafo 2, TUE e l'articolo 1, paragrafo 3, lettera c), della direttiva 2018/1972

devono essere interpretati nel senso che una misura che prescrive l'autorizzazione di hardware e software per la fornitura di una rete o di un servizio di comunicazione elettronica pubblici o accessibili al pubblico non è esclusa dall'ambito di applicazione della direttiva 2018/1972, anche se tale misura è stata adottata al fine di tutelare gli interessi della sicurezza nazionale.

3) L'articolo 12, paragrafo 1, della direttiva 2018/1972

deve essere interpretato nel senso che un insieme di disposizioni legislative e regolamentari nazionali che prescrive l'autorizzazione di un'autorità amministrativa per l'uso di hardware e software nella fornitura di reti e servizi di comunicazione elettronica costituisce una limitazione della libertà di fornire tali reti e servizi, ai sensi di detta disposizione.

Una simile limitazione può essere giustificata dai motivi previsti all'articolo 52, paragrafo 1, TFUE.4) L'articolo 12, paragrafo 1, della direttiva 2018/1972

deve essere interpretato nel senso che la mancata comunicazione alla Commissione europea di una limitazione della libertà di fornire reti di comunicazione elettronica non comporta l'inapplicabilità della normativa nazionale non comunicata.

5) L'articolo 12, paragrafo 1, della direttiva 2018/1972 e il principio di proporzionalità

devono essere interpretati nel senso che esigono che disposizioni legislative e regolamentari nazionali, che impongono di ottenere un'autorizzazione preventiva d'uso di hardware e software al fine di tutelare la sicurezza delle reti e dei servizi di comunicazione elettronica, obblighino gli organismi abilitati a decidere in merito alla concessione di una siffatta autorizzazione a valutare se gli hardware e software di cui trattasi, di cui si chiede l'uso, presentino un rischio reale per la sicurezza della rete, il che può includere la presa in considerazione dell'uso cui tali apparecchiature sono destinate, nonché delle questioni se i rischi associati allo Stato di stabilimento del produttore si riflettano sullo quest'ultimo e se i rischi associati al produttore si riflettano sugli specifici hardware e software.

6) Una limitazione dell'uso di hardware o software preesistenti, in una rete di comunicazione elettronica, all'introduzione dell'obbligo di autorizzazione d'uso, in forza del quale l'uso è concesso per un periodo inferiore alla vita utile di tale hardware o software, non costituisce una privazione della proprietà ai sensi dell'articolo 17, paragrafo 1, seconda frase, della Carta dei diritti fondamentali dell'Unione europea.

---

1 Lingua originale: l'inglese.

---

2 Direttiva (UE) del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche (GU 2018, L 321, pag. 36).

---

3 V., in tal senso, Sendin, A., Sanchez-Fornie, M.A., Berganza, I., Simon, J., Irritoa, I., *Telecommunication Networks for the Smart Grid*, Artech House, Boston, 2016, pag. 176. Data la sua importanza fondamentale per l'infrastruttura di telecomunicazioni nel suo complesso, la rete principale è talvolta definita come la «dorsale» o il «cervello» di una rete mobile. V., in generale, su questo punto il Centro di eccellenza per la difesa informatica cooperativa della NATO, che ha descritto la rete principale come «infrastruttura fondamentale e quindi (…) un interesse nazionale essenziale, con implicazioni per la sicurezza nazionale». V. Centro di eccellenza per la difesa informatica cooperativa della NATO, Kaska, K., Beckvard, H. e Minárik, T., «Huawei, 5G and China as a Security Threat», 2019, pag. 15, disponibile all'indirizzo: https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf.

---

4 V., ad esempio, in Germania, Ufficio federale per la sicurezza informatica, «5G Risk Analysis, Framework Document: Methodology, Risk Scenarios and Results», 2025, pag. 21, in cui viene spiegato che «la rete di accesso radio (RAN) contiene stazioni base 5G (…) con un'interfaccia radio (…) che fornisce connettività ai dispositivi mobili» (disponibile all'indirizzo: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/5G/5G_Framework_Document.pdf?__blob=publicationFile&v= 4).

---

5 In alcuni Stati membri le reti 2G e 3G sono già in fase di disattivazione; v., ad esempio, nel caso dell'Irlanda, Commissione per la regolamentazione delle comunicazioni, «2G/3G Switch off: Guidance for Mobile Network Operators», ComReg 24/61, 30 luglio 2024, disponibile all'indirizzo: https://www.comreg.ie/media/2024/07/ComReg-2461.pdf.

---

6 La Commissione ha manifestato tale posizione già nel 2016, e in seguito l'ha approfondita. V. comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, «Il 5G per l'Europa: un piano d'azione», COM(2016) 588 final, pag. 4, in cui la Commissione afferma che «[p]er situarsi in una posizione di leadership e trarre profitto fin dall'inizio dalle nuove opportunità di mercato offerte dal 5G, non solo nel settore delle telecomunicazioni ma nel complesso dell'economia e della società, l'Europa ha bisogno di un calendario ambizioso per l'introduzione del 5G».

---

7 Nel punto 2, lettera a), della raccomandazione (UE) 2019/534 della Commissione, del 26 marzo 2019, Cibersicurezza delle reti 5G (GU 2019, L 88, pag. 42) (in prosieguo: la «raccomandazione sulla cibersicurezza»), la Commissione definisce «reti 5G» come «un insieme di tutti gli elementi pertinenti delle infrastrutture di rete per le tecnologie delle comunicazioni mobili e senza fili utilizzati per la connettività e per servizi a valore aggiunto con caratteristiche di prestazione avanzate, quali capacità e velocità di trasmissione dei dati molto elevate, comunicazioni a bassa latenza, affidabilità ultra-elevata o capacità di supportare un numero elevato di dispositivi connessi. Tale insieme può includere elementi di rete tradizionali basati sulle precedenti generazioni di tecnologie delle comunicazioni mobili e senza fili, come il 4G o il 3G. Le reti 5G dovrebbero essere intese in modo da includere tutte le parti pertinenti della rete».

---

8 V., ad esempio, la relazione speciale della Corte dei conti europea del 2022, in cui si afferma che «[a] fine 2018, si stima vi fossero 22 miliardi di dispositivi connessi in uso nel mondo [e] che tale cifra aumenterà fino a circa 50 miliardi entro il 2030, creando un'enorme rete di dispositivi interconnessi includenti tutto, dagli smartphone agli apparecchi da cucina. Si prevede che entro il 2030 il consumo mondiale di dati balzerà dai 12 exabyte al mese di traffico su reti mobili nel 2017 a oltre 5 000 exabyte». V. Corte dei conti europea, «L'introduzione del 5G nell'UE: vi sono ritardi nel dispiegamento delle reti e le questioni di sicurezza rimangono irrisolte», Relazione speciale n. 03/2022, Ufficio delle pubblicazioni dell'Unione europea, Lussemburgo, 2022,

pag. 7, disponibile all'indirizzo: https://www.eca.europa.eu/Lists/ECADocuments/SR22_03/SR_Security-5G-networks_IT.pdf.

9 Occorre osservare che, sebbene la decisione di rinvio e le osservazioni della ricorrente menzionino il 23 marzo 2022 come data di presentazione della richiesta di autorizzazione da parte della ricorrente, secondo le osservazioni del governo estone e alcune parti del fascicolo nazionale, compresa la decisione n. 1-7/22-436 del 25 novembre 2022 del TTJA, tale richiesta è datata 18 marzo 2022.

10 Una traduzione in inglese di tale testo può essere consultata al seguente indirizzo: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/528102025002/consolide.

11 Detti 12 criteri sono i seguenti: 1) il produttore o fornitore di servizi di manutenzione o di assistenza ha la propria sede legale o amministrazione centrale in un paese (…) che non è membro dell'Unione europea, dell'Organizzazione del Trattato del Nord Atlantico [(NATO)] o dell'Organizzazione per la cooperazione e lo sviluppo economici [(OCSE)]; 2) i principi dello Stato di diritto democratico non sono rispettati o i diritti umani non sono rispettati nel paese di residenza del produttore o del fornitore di servizi di manutenzione o di assistenza; 3) la proprietà intellettuale, i dati personali o i segreti commerciali di persone di altri paesi non sono protetti nel paese di residenza del produttore o del fornitore di servizi di manutenzione o di assistenza; 4) il paese di residenza del produttore o del prestatore di servizi di manutenzione o di assistenza mostra un comportamento aggressivo nel ciberspazio; 5) gli Stati membri dell'Unione europea, della NATO o dell'OCSE hanno attribuito attacchi informatici al paese di residenza del produttore o del fornitore di servizi di manutenzione o di assistenza; 6) il produttore o il fornitore di servizi di manutenzione o assistenza è sottoposto all'autorità del governo o dello Stato del paese di residenza o di un altro paese straniero che non dispone di un controllo giurisdizionale indipendente; 7) il paese di residenza del produttore o del fornitore di servizi di manutenzione o di assistenza o un altro paese straniero può obbligarlo ad agire in un modo che rappresenta un rischio per la sicurezza nazionale dell'Estonia; 8) le attività economiche del produttore o del fornitore di servizi di manutenzione o assistenza non si fondano su una concorrenza basata sul mercato o non sono state create a tal fine condizioni adeguate nel paese di residenza; 9) l'assetto proprietario e la struttura organizzativa o di gestione del produttore o del fornitore di servizi di manutenzione o assistenza non sono trasparenti; 10) il finanziamento del produttore o del prestatore di servizi di manutenzione o assistenza non è trasparente; 11) i prodotti o servizi del produttore o fornitore di servizi di manutenzione o assistenza includono elementi di vulnerabilità, senza che siano state attuate misure di sicurezza adeguate per eliminarli; 12) il produttore o il prestatore di servizi di manutenzione o assistenza non è in grado di assicurare le consegne di prodotti o di servizi in modo continuato, salvo il caso di forza maggiore».

12 Secondo il testo dell'articolo 196^5 dell'ESS, ciò riguarda «il 5G [non autonomo] o uno standard di rete di comunicazioni mobili di più nuova generazione».

13 Dal testo dell'articolo 196^5 dell'ESS risulta, a mio parere, che dopo il 31 dicembre 2025 non saranno rilasciate ulteriori autorizzazioni per la tecnologia 5G che è stata ritenuta un rischio per la sicurezza nazionale, mentre l'autorizzazione per il proseguimento dell'uso di hardware e software 2G, 3G e 4G, anche nei casi in cui sia stato riscontrato un rischio per la sicurezza nazionale, potrà essere richiesta dopo il 31 dicembre 2029.

14 Ai sensi dell'articolo 87^3, paragrafo 2, dell'ESS, l'hardware o il software utilizzato in una rete di comunicazione può minacciare la sicurezza nazionale a causa dell'elevato rischio derivante dal produttore o dal fornitore di servizi di manutenzione o assistenza (punto 1) o a causa del rischio connesso alle caratteristiche tecniche o alla configurazione dell'hardware o del software (punto 2).

15 V. la precedente nota a piè di pagina. In udienza, il governo estone ha spiegato che esempi dei tipi di rischi individuati riguardavano il potenziale di spionaggio, l'uso illecito di informazioni e dati e la compromissione di servizi di cruciale importanza.

16 Direttiva del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (GU 2015, L 241, pag. 1).

17 V., in tal senso, articolo 1, paragrafo 1, del CECE. In tale misura, il CECE rifonde una serie di atti adottati sotto forma di pacchetto nel marzo 2002, che disciplinavano in precedenza le comunicazioni elettroniche al fine di adeguare il quadro normativo all'evoluzione delle tecnologie e del mercato. V., in tal senso, sentenza del 27 febbraio 2025, T - 2 (C-562/23, EU:C:2025:126, punto 37 e giurisprudenza citata).

18 Come stabilito al considerando 5 del CECE, la libera prestazione delle reti e dei servizi di comunicazione elettronica dovrebbe essere soggetta soltanto alle condizioni stabilite in tale direttiva.

19 V. articolo 2, punto 1, del CECE.

20 Il corsivo è mio.

21 V. articolo 2, punto 1, del CECE.

22 V. articolo 2, punto 4, del CECE.

23 La nozione di «reti di comunicazione elettronica» è definita all'articolo 2, punto 1, del CECE come: «i sistemi di trasmissione, basati o meno su un'infrastruttura permanente o una capacità di amministrazione centralizzata, e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti mobili e fisse (a commutazione di circuito e a commutazione di pacchetto, compresa [l]nternet), i sistemi per il trasporto via cavo della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti utilizzate per la diffusione radiotelevisiva, e le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato».

24 V., in tal senso, sentenze del 5 giugno 2019, *Skype Communications* (C-142/18, EU:C:2019:460, punto 49) e del 13 giugno 2019, *Google* (C-193/18, EU:C:2019:498, punti 34, 35 e 41).

25 L'articolo 4, paragrafo 2, TUE fa riferimento alla «sicurezza nazionale», mentre l'articolo 1, paragrafo 3, lettera c), del CECE utilizza le espressioni «ordine pubblico» e «pubblica sicurezza». Tuttavia, ad esempio, il considerando 6 del CECE utilizza l'espressione «interessi essenziali in materia di sicurezza», oltre a riferimenti all'«ordine pubblico» e alla «pubblica sicurezza», nell'ambito della formulazione «fa salva». Poiché nulla nel testo del CECE, nel suo obiettivo o nei suoi lavori preparatori consente di ritenere diversamente [v. proposta di direttiva del Parlamento europeo e del Consiglio che istituisce il codice europeo delle comunicazioni elettroniche (COM(2016) 590 final/ 2)], ritengo che la terminologia utilizzata nel testo dell'articolo 1, paragrafo 3, lettera c), del CECE debba essere interpretata nel senso che include le nozioni di «sicurezza nazionale» o di «interessi essenziali in materia di sicurezza». Ciò sarebbe conforme anche ai termini utilizzati nella direttiva che ha

preceduto il CECE, che nei suoi considerando (sebbene in assenza di un articolo specifico in tal senso) già conteneva una siffatta formulazione. V. considerando 7 della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro) (GU 2002, L 108, pag. 33).

26 V., per esempio, sentenze del 26 ottobre 1999, *Sirdar* (C-273/97, EU:C:1999:523, punto 15); del 6 ottobre 2020, *Privacy International* (C-623/17, EU:C:2020:790, punto 44 e giurisprudenza citata), e del 15 luglio 2021, *Ministrstvo za obrambo* (C-742/19, EU:C:2021:597, punto 40 e giurisprudenza citata).

27 V., di recente, sentenza del 29 luglio 2024, *protectus* (C-185/23, EU:C:2024:657, punto 62 e giurisprudenza citata).

28 In tal senso, il presente procedimento costituisce un esempio interessante della «securitizzazione» del diritto dell'Unione. Sullo sviluppo di un «duopolio di sicurezza» tra gli Stati membri e le istituzioni politiche dell'Unione, in cui gli orientamenti politici confluiscono nelle azioni a livello nazionale e dell'Unione, v. Pilniok, A., «Governance of the European Security Union», in Dietrich, J.H., e Pilniok, A., *European Security Union: Law and Policies*, Beck/Hart/Nomos, 2024, pagg. 18 e 19.

29 V., in particolare, la raccomandazione del 2019 sulla cibersicurezza e la comunicazione della Commissione: Attuazione del pacchetto di strumenti per la cibersicurezza del 5G C (2023) 4049 final (in prosieguo: la «comunicazione sull'attuazione del pacchetto di strumenti 5G»).

30 V. gruppo di cooperazione NIS, «EU coordinated risk assessment of the cybersecurity of 5G networks» (valutazione dei rischi coordinata dell'UE della cibersicurezza delle reti 5G), 2019 (in prosieguo: la «valutazione dei rischi coordinata»), disponibile all'indirizzo: https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security. V. anche gruppo di cooperazione NIS, «Cybersecurity of 5G networks, EU Toolbox of risk mitigating measures» (cibersicurezza delle reti 5G, pacchetto di strumenti dell'UE sulle misure di attenuazione), 2020 (in prosieguo: il «pacchetto di strumenti sul 5G»), disponibile all'indirizzo: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

31 Sentenza del 15 luglio 2021 (C-742/19, EU:C:2021:597).

32 Direttiva del Parlamento europeo e del Consiglio, del 4 novembre 2003 (GU 2003, L 299, pag. 9).

33 V. sentenza del 15 luglio 2021, Ministrstvo za obrambo (C-742/19, EU:C:2021:597, punto 75).

34 Il governo francese sottolinea altresì che non è ovvio che un sistema di autorizzazione preventiva per hardware e software, come quello di cui trattasi nel procedimento principale, incida sulla possibilità di fornire tali reti o servizi. A suo avviso, tale sistema non impone in alcun modo agli operatori di telecomunicazioni di ottenere un'autorizzazione per poter esercitare l'attività di fornitura di reti e di servizi di comunicazione elettronica in generale.

35 Il corsivo è mio.

36 Sebbene l'articolo 12, paragrafo 1, del CECE contenga una formulazione secondo cui gli Stati membri non «impediscono» la libera fornitura di reti e di servizi di comunicazione elettronica, ritengo che tale espressione debba essere intesa in un'accezione più ampia, nel senso che vieta agli Stati membri di imporre *qualsiasi tipo di impedimento* alla loro fornitura. Ciò deriverebbe dall'obiettivo del CECE di istituire un mercato interno delle reti e dei servizi di comunicazione elettronica. Tale conclusione può essere tratta anche dalle diverse versioni linguistiche dell'articolo 12, paragrafo 1, del CECE, che utilizzano termini significanti sia «impedire» che «prevenire»: si confrontino, in tal senso, ad esempio, la versione in lingua tedesca, che fa riferimento a «hindern»; la versione in lingua spagnola, che fa riferimento a «no impedirán»; la versione in lingua francese, che fa riferimento a «n'empêchent pas»; o la versione in lingua croata, che fa riferimento a «ne smiju sprečavati».

37 Si immagini una situazione in cui uno Stato membro decida che, al fine di garantire la sicurezza delle reti, qualsiasi hardware e software utilizzato in tali reti debba essere prodotto da imprese stabilite in tale Stato. Una siffatta misura protezionistica sarebbe manifestamente contraria alla libera prestazione delle reti e dei servizi, ma sarebbe giustificabile se il CECE fosse interpretato in modo tale da considerare automaticamente accettabile ed escludere da un ulteriore esame qualsiasi misura adottata al fine di raggiungere l'obiettivo della sicurezza delle reti e dei servizi.

38 V., ad esempio, sentenza del 23 febbraio 1995, *Bordessa e a.* (C-358/93 e C-416/93, EU:C:1995:54, punto 25).

39 V., ad esempio, sentenza del 4 dicembre 1986, *Commissione/Germania* (205/84, EU:C:1986:463, punto 28).

40 V., ad esempio, sentenza del 14 marzo 2000, *Église de scientologie* (C-54/99, EU:C:2000:124, punto 14).

41 V., ad esempio, sentenza del 1º giugno 2010, *Blanco Pérez e Chao Gómez* (C-570/07 e C-571/07, EU:C:2010:300, punto 54).

42 Il governo estone fa riferimento alla comunicazione tecnica di tale bozza, ricevuta dalla Commissione il 20 ottobre 2020, disponibile all'indirizzo: https://technical-regulation-information-system.ec.europa.eu/en/notification/15441.

43 V. in particolare, sentenze del 30 aprile 1996, *CIA Security International* (C-194/94, EU:C:1996:172, punto 54), e del 21 dicembre 2023, *Papier Mettler Italia* (C-86/22, EU:C:2023:1023, punto 44).

44 V., *ex multis*, sentenza del 15 luglio 2021, *Ministrstvo za obrambo* (C-742/19, EU:C:2021:597, punto 31 e giurisprudenza citata).

45 V., a tal riguardo, i considerando 5 e 37 della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (GU 2022, L 333, pag. 80) (in prosieguo: la «direttiva NIS 2»).

46 V., in tal senso, sentenza del 20 giugno 2002, *Radiosistemi* (C-388/00 e C-429/00, EU:C:2002:390, punto 44). In ogni caso, già a partire dalla sentenza del 10 luglio 1984, *Campus Oil e a.* (72/83, EU:C:1984:256, in

particolare punti da 34 a 36), risulta chiaro che la giurisprudenza interpreta la nozione di pubblica sicurezza nel senso che essa trascende l'ordine pubblico e il ricorso alle forze di polizia e dell'esercito; in tale sentenza, la Corte ha dichiarato che la suddetta nozione può riferirsi anche ad altri tipi di minacce per le istituzioni di uno Stato membro, per i suoi servizi pubblici essenziali e, più in generale, per le esigenze della società.

47 V. paragrafi da 32 a 42 delle presenti conclusioni.

48 V., *ex multis*, sentenze del 14 marzo 2000, *Église de scientologie* (C-54/99, EU:C:2000:124, punto 17 e giurisprudenza citata), e del 18 giugno 2020, *Commissione/Ungheria (Trasparenza associativa)* (C-78/18, EU:C:2020:476, punto 91 e giurisprudenza citata).

49 V., per analogia, sentenza del 3 settembre 2008, *Kadi e Al Barakaat International Foundation/Consiglio e Commissione* (C-402/05 P e C-415/05 P, EU:C:2008:461, punto 343) (in cui si precisa che un provvedimento non può sottrarsi a ogni controllo da parte dei giudici dell'Unione per il solo fatto che l'atto che lo prevede riguarda la sicurezza nazionale).

50 V., per analogia, sentenza del 26 febbraio 2019, *X (Società intermedie stabilite in paesi terzi)* (C-135/17, EU:C:2019:136, punto 90 e giurisprudenza citata).

51 V., in tal senso, sentenze del 14 marzo 2000, *Église de scientologie* (C-54/99, EU:C:2000:124, punto 22) e del 18 giugno 2020, *Commissione/Ungheria (Trasparenza associativa)* (C-78/18, EU:C:2020:476, punti 86 e 93).

52 V., per analogia, sentenza del 10 marzo 2016, *Safe Interenvíos* (C-235/14, EU:C:2016:154, punto 104) (in cui si spiega che, in materia di riciclaggio di denaro, la valutazione di rischio elevato di un cliente può riguardare il tipo di cliente, il paese, il prodotto o la transazione di cui trattasi).

53 V., a tal proposito, nota a piè di pagina 11 *supra*.

54 V., per analogia, sentenza del 21 novembre 1991, *Technische Universität München* (C-269/90, EU:C:1991:438, punti 13 e 14).

55 V., in tal senso, sentenza del 4 giugno 2013, *ZZ* (C-300/11, EU:C:2013:363, punto 57 e giurisprudenza citata).

56 Tale pacchetto di strumenti deriva da uno degli obiettivi fissati dalla Commissione nella sua raccomandazione sulla cibersicurezza (v. punto 1, lettera c) della stessa, che stabilisce che il gruppo di cooperazione NIS «[individui] un'eventuale serie comune di misure da adottare per attenuare i rischi di cibersicurezza relativi alle infrastrutture alla base dell'ecosistema digitale, in particolare le reti 5G».

57 V. nota a piè di pagina 30 *supra*. Tale gruppo costituisce un comitato istituito sulla base dell'articolo 11, paragrafo 1, della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU 2016, L 194, pag. 1). Tale direttiva è stata nel frattempo sostituita dalla direttiva NIS 2, ma il comitato continua ad esistere (v. articolo 14, paragrafo 1, della direttiva NIS 2).

58 V. comunicazione sull'attuazione del pacchetto di strumenti sul 5G, pag. 2.

59 V. comunicazione sull'attuazione del pacchetto di strumenti sul 5G, pag. 2. Per criteri di vulnerabilità simili, relativi al fornitore, v. anche la pag. 42 del pacchetto di strumenti sul 5G.

60 V. sentenza del 10 luglio 2025, *INTERZERO e a.* (C-254/23, EU:C:2025:569, punto 144 e giurisprudenza citata). A tal riguardo, v. anche sentenza del 5 maggio 2022, *BPC Lux 2 e a.* (C-83/20, EU:C:2022:346, punto 38 e giurisprudenza citata).

61 V., in tal senso, sentenza del 10 luglio 2025, INTERZERO e a. (C-254/23, EU:C:2025:569, punti 145 e 146 nonché giurisprudenza citata).

62 V., in tal senso, sentenza del 10 settembre 2024, *Neves 77 Solutions* (C-351/22, EU:C:2024:723, punti 82 e 88 nonché giurisprudenza citata).

63 V., per analogia, sentenza del 10 luglio 2025, *INTERZERO e a.* (C-254/23, EU:C:2025:569, punto 146 e giurisprudenza citata) (in cui viene spiegato che «gli interessi connessi allo sfruttamento di una licenza costituiscono interessi patrimoniali che richiedono la tutela conferita nel citato articolo[1 del protocollo n. 1 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali]», cosicché «la revoca *ex lege* di un'autorizzazione che consente al suo titolare di esercitare un'attività economica costituisce una limitazione al diritto di proprietà garantito da tale articolo che rientra, in quanto misura di regolamentazione dell'uso dei beni, nel secondo comma di detto articolo»).

64 V., in tal senso, sentenza del 10 luglio 2025, *INTERZERO e a.* (C-254/23, EU:C:2025:569, punto 155 e giurisprudenza citata).

65 V., in tal senso, sentenza del 10 luglio 2025, INTERZERO e a. (C-254/23, EU:C:2025:569, punti 155 e 156, nonché giurisprudenza citata).

66 V., da ultimo, sentenza del 18 dicembre 2025, *Slagelse Almennyttige Boligselskab, Afdeling Schackenborgvænge* (C-417/23, EU:C:2025:1017, punto 168 e giurisprudenza citata).

67 V., in tal senso, sentenza del 10 luglio 2025, *INTERZERO e a.* (C-254/23, EU:C:2025:569, punto 158 e giurisprudenza citata).