CONCLUSIONI DELL'AVVOCATO GENERALE

GIOVANNI PITRUZZELLA

presentate il 21 gennaio 2020 (1)

Causa C-746/18

H.K.

contro

Prokuratuur

[domanda di pronuncia pregiudiziale proposta dalla Riigikohus (Corte suprema, Estonia)]

«Rinvio pregiudiziale – Trattamento dei dati personali nel settore delle comunicazioni elettroniche – Riservatezza delle comunicazioni – Fornitori di servizi di comunicazione elettronica – Conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione – Indagini penali – Accesso dell'autorità inquirente ai dati conservati riferiti a periodi compresi tra un giorno e un anno – Autorizzazione concessa dal pubblico ministero – Utilizzo dei dati nel contesto del processo penale quali mezzi di prova – Direttiva 2002/58/CE – Articolo 1, paragrafo 3, articolo 3, e articolo 15, paragrafo 1 – Carta dei diritti fondamentali dell'Unione europea – Articoli 7, 8, 11 e 52, paragrafo 1»

I. Introduzione

1. La domanda di pronuncia pregiudiziale in esame verte sull'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (2), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009 (3), letto alla luce degli articoli 7, 8, 11 e 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea (4).

2. Tale domanda è stata presentata nel contesto di un procedimento penale promosso a carico di H.K., per il motivo che quest'ultima avrebbe commesso vari furti, utilizzato una carta bancaria appartenente ad un'altra persona e commesso atti di violenza nei confronti di una persona che partecipava a un procedimento giudiziario.

3. I verbali su cui si basa la contestazione di tali reati sono stati redatti, in particolare, sulla base di dati personali creati nel contesto della fornitura di servizi di comunicazione elettronica. La Riigikohus (Corte suprema, Estonia) esprime dubbi in ordine alla compatibilità con il diritto dell'Unione delle condizioni in base alle quali i servizi inquirenti hanno avuto accesso a tali dati.

4. Tali dubbi riguardano, in primo luogo, la questione se la durata del periodo cui si riferiscono i dati ai quali i servizi inquirenti hanno avuto accesso costituisca un criterio che permette di valutare la gravità dell'ingerenza rappresentata da tale accesso nei diritti fondamentali delle persone interessate.

5. In secondo luogo, il giudice del rinvio intende sapere se il Prokuratuur (pubblico ministero, Estonia), tenuto conto delle varie funzioni affidategli dalla normativa estone, costituisca un'autorità amministrativa «indipendente» ai sensi della sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (5).

II. Contesto normativo

A. Direttiva 2002/58

6. In forza dell'articolo 1, paragrafo 3, della direttiva 2002/58, quest'ultima «non si applica alle attività che esulano dal campo di applicazione del trattato che istituisce la Comunità europea, quali quelle disciplinate dai titoli V e VI del trattato sull'Unione europea né, comunque, alle attività riguardanti la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) o alle attività dello Stato in settori che rientrano nel diritto penale».

7. Inoltre, l'articolo 15, paragrafo 1, di tale direttiva, stabilisce che «[g]li Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE [(6)], una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai

principi generali del diritto [dell'Unione], compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea».

B. Diritto estone

1. Legge sulla comunicazione elettronica

8. L'elektroonilise side seadus (legge sulla comunicazione elettronica) (7), dell'8 dicembre 2004, nella sua versione applicabile alla controversia di cui al procedimento principale, all'articolo 1111, intitolato «Obbligo di conservazione dei dati», dispone quanto segue:

«(...)

(2) I fornitori di servizi di telefonia fissa e mobile nonché di servizi di rete di telefonia fissa e mobile sono obbligati a conservare i seguenti dati:

1) il numero telefonico del chiamante nonché il nome e il recapito dell'abbonato;

2) il numero telefonico del chiamato nonché il nome e il recapito dell'abbonato;

3) in caso di utilizzo di servizi supplementari come l'inoltro o il trasferimento di chiamata, il numero selezionato nonché il nome e il recapito dell'abbonato;

4) la data e l'orario di inizio e fine di una chiamata;

5) il servizio di telefonia fissa o mobile utilizzato;

6) l'identità utente mobile internazionale (International Mobile Subscriber Identity – IMSI) della linea chiamante e della linea chiamata;

7) l'identificatore internazionale apparecchiature mobili (International Mobile Equipment Identity – IMEI) della linea chiamante e della linea chiamata;

8) l'etichetta di ubicazione all'inizio della chiamata;

9) dati per identificare l’ubicazione geografica delle cellule facendo riferimento alle loro etichette di ubicazione nel periodo in cui vengono conservati i dati sulle comunicazioni;

10) nel caso di servizi prepagati anonimi, la data e l’ora dell’attivazione iniziale della carta e l’etichetta di ubicazione dalla quale è stata effettuata l’attivazione;

(...)

(4) I dati indicati nei paragrafi 2 e 3 del presente articolo vengono conservati per un periodo di un anno dalla data della comunicazione, se tali dati vengono creati o trattati nell’ambito della fornitura di un servizio di comunicazione (...)

(...)

(11) I dati indicati nei paragrafi 2 e 3 del presente articolo vengono comunicati:

1) ai sensi del kriminaalmenetluse seadustik [codice di procedura penale (8)], a un’autorità inquirente, a un’autorità autorizzata ad applicare misure di sorveglianza, al pubblico ministero e al giudice;

(...)».

2. Codice di procedura penale

9. L’articolo 17 del codice di procedura penale, nella sua versione applicabile alla controversia di cui al procedimento principale, intitolato «Parti del procedimento giudiziario», al paragrafo 1 dispone quanto segue:

«Sono parti del procedimento giudiziario: il pubblico ministero (...)».

10. Ai sensi dell’articolo 30 del codice di procedura penale, intitolato «Il pubblico ministero nel procedimento penale»:

«(1) Il pubblico ministero dirige il procedimento istruttorio, di cui assicura la legittimità e l'efficacia, e rappresenta la pubblica accusa in giudizio.

(2) I poteri del pubblico ministero nel procedimento penale vengono esercitati, in nome del pubblico ministero, da un procuratore, il quale agisce in modo indipendente ed è soggetto soltanto alla legge».

11. L'articolo 901 del codice di procedura penale, intitolato «Richiesta di dati a un'impresa di comunicazioni», ai suoi paragrafi 2 e 3 prevede quanto segue:

«(2) L'autorità inquirente, nel corso del procedimento istruttorio, con l'autorizzazione del pubblico ministero ovvero, nel corso del processo, con l'autorizzazione del giudice, può richiedere a un fornitore di servizi di comunicazione elettronica i dati elencati nell'articolo 1111, paragrafi 2 e 3, della legge sulla comunicazione elettronica, non menzionati nel precedente paragrafo 1. Nell'autorizzazione della richiesta viene specificato il periodo con riferimento al quale la richiesta dei dati viene concessa, con l'esatta indicazione della data.

(3) Ai sensi del presente articolo, i dati possono essere richiesti soltanto laddove ciò sia indispensabile al fine di raggiungere lo scopo del procedimento penale».

12. L'articolo 211 del codice di procedura penale, intitolato «Scopo del procedimento istruttorio», è così formulato:

«(1) Lo scopo del procedimento istruttorio è quello di raccogliere prove e di predisporre le altre condizioni necessarie allo svolgimento di un processo.

(2) Nel procedimento istruttorio l'autorità inquirente e il pubblico ministero verificano gli elementi a carico e quelli a discarico raccolti nei confronti del sospettato o dell'indagato».

3. Legge relativa al pubblico ministero

13. La prokuratuuriseadus (legge relativa al pubblico ministero) (9), del 22 aprile 1998, nella sua versione applicabile alla controversia di cui al procedimento principale, all'articolo 1, intitolato «Pubblico ministero», dispone quanto segue:

«(1) Il pubblico ministero è un'autorità soggetta alla sfera di competenza del Justiitsministeeriumi [Ministero della Giustizia, Estonia], la quale partecipa alla pianificazione delle misure di sorveglianza

ai fini della lotta e dell'accertamento di reati, dirige il procedimento istruttorio, di cui assicura la legittimità e l'efficacia, rappresenta la pubblica accusa nel processo ed esercita le ulteriori funzioni assegnategli dalla legge.

(11) Il pubblico ministero, nell'esercizio delle funzioni assegnategli dalla legge, è indipendente e agisce conformemente alla presente legge, alle altre leggi e agli atti normativi emanati sulla base di tali leggi.

(...)».

14. L'articolo 2 della legge relativa al pubblico ministero, intitolato «Procuratore», al paragrafo 2 così recita:

«Il procuratore, nell'esercizio delle proprie funzioni, è indipendente e agisce esclusivamente secondo la legge e secondo il proprio convincimento».

III. Fatti, procedimento principale e questioni pregiudiziali

15. Con sentenza del 6 aprile 2017, H.K. è stata condannata dal Viru Maakohus (Tribunale di primo grado di Viru, Estonia), a una pena detentiva di due anni per aver commesso, nel periodo tra il 4 agosto 2015 e il 1° febbraio 2016, otto furti di prodotti alimentari e di altri beni materiali di un valore compreso tra EUR 3 e 40 nonché di somme di denaro di importi compresi tra EUR 5,20 e 2 100, per aver utilizzato la carta bancaria di un'altra persona al fine di prelevare denaro da un distributore automatico di banconote, causando a tale persona un danno di EUR 3 941,82 e per aver commesso atti di violenza nei confronti di una parte di un procedimento giudiziario (10).

16. Ai fini della condanna di H.K. per tali reati, il Viru Maakohus (Tribunale di primo grado di Viru) si è fondato, tra l'altro, su vari verbali redatti sulla base di dati relativi a comunicazioni elettroniche, dati contemplati dall'articolo 1111, paragrafo 2, della legge sulla comunicazione elettronica, che l'autorità inquirente aveva raccolto presso un fornitore di servizi di telecomunicazioni nel corso del procedimento istruttorio, dopo aver ottenuto, ai sensi dell'articolo 901, paragrafo 2, del codice di procedura penale, autorizzazioni concesse da un procuratore del Viru Ringkonnaprokuratuur (procura distrettuale di Viru, Estonia).

17. Così, il 2 novembre 2015, un procuratore della procura distrettuale di Viru ha autorizzato l'autorità inquirente a ordinare all'impresa di telecomunicazioni di fornire i dati di cui all'articolo 1111, paragrafo 2, della legge sulla comunicazione elettronica, al fine di accertare la trasmissione, in data 21 settembre 2015, di chiamate e messaggi mediante due numeri di telefono cellulare di H.K., la loro durata, la modalità di trasmissione, i dati personali e l'ubicazione del chiamante o mittente e del chiamato o destinatario.

18. Sulla base dei dati ottenuti dall'impresa di telecomunicazioni in virtù di tale autorizzazione, l'autorità inquirente, in data 4 novembre 2015, ha redatto un verbale nel quale erano indicati i ripetitori telefonici nel cui raggio d'azione era stato utilizzato il numero di abbonato usato da H.K. il 21 settembre 2015 dopo le ore 19:00. Il pubblico ministero, con tale verbale, unitamente ad altri mezzi di prova, ha inteso dimostrare in giudizio che H.K. era l'autrice del furto perpetrato il 21 settembre 2015.

19. In data 25 febbraio 2016 un procuratore della procura distrettuale di Viru ha autorizzato l'autorità inquirente a ordinare all'impresa di telecomunicazioni di fornire, ai fini dell'indagine su un reato di cui all'articolo 303, paragrafo 1, del Karistusseadustik (codice penale) (11), i dati di cui all'articolo 1111, paragrafo 2, della legge sulla comunicazione elettronica, sui sette numeri di abbonato utilizzati da H.K. nel periodo compreso tra il 1° marzo 2015 ed il 19 febbraio 2016.

20. In data 15 marzo 2016 l'autorità inquirente ha redatto un verbale sulla base dei dati ottenuti dall'impresa di telecomunicazioni in virtù di tale autorizzazione, nel quale erano indicati i giorni in cui H.K. aveva chiamato i coimputati ed aveva ricevuto chiamate dei medesimi, nonché le date in cui H.K. aveva inviato loro messaggi e ne aveva ricevuti da essi. Il pubblico ministero, con detto verbale, unitamente ad altri mezzi di prova, ha inteso dimostrare in giudizio che H.K., dalla primavera del 2015, aveva ripetutamente minacciato per telefono i coimputati.

21. Il 20 aprile e il 6 maggio 2016 l'autorità inquirente ha redatto altresì verbali relativi ai dati ottenuti dall'impresa di telecomunicazioni in virtù di tale autorizzazione. Nei verbali sono annotate le stazioni base nella cui copertura, in data 4, 27 e 31 agosto 2015 nonché dal 1° al 3 settembre 2015, sono partite chiamate dai sei numeri di abbonato utilizzati da H.K. e sono giunte chiamate a questi. Il pubblico ministero, con detti verbali, unitamente ad altri mezzi di prova, ha inteso dimostrare in giudizio che H.K. era l'autrice dei sei furti perpetrati nei giorni sopra indicati.

22. In data 20 aprile 2016, l'autorità inquirente ha redatto un verbale nel quale erano riportati i dati di due numeri di abbonato utilizzati da H.K. In particolare, dal verbale risultano le stazioni base nel cui raggio di copertura, nel periodo compreso tra il 16 ed il 19 gennaio 2015, sono partite chiamate da tali numeri di abbonato e sono giunte chiamate ai medesimi. Sulla base di detto verbale, unitamente ad altri mezzi di prova, il pubblico ministero ha inteso dimostrare che H.K. era la persona che, dal 17 al 19 gennaio 2015, aveva prelevato denaro contante con la carta bancaria della vittima da un distributore automatico di banconote.

23. I dati su cui si basa il verbale sono stati ottenuti dall'impresa di telecomunicazioni grazie ad autorizzazioni rilasciate in data 28 gennaio e 2 febbraio 2015 in un altro procedimento penale da un procuratore della procura distrettuale di Viru. Tale procedimento penale riguardava reati di cui all'articolo 200, paragrafo 2, punti 7, 8 e 9, del codice penale, ovvero due furti che erano stati commessi da un gruppo, il 23 e 27 gennaio 2015, a mano armata e con violazione di domicilio. In virtù delle suddette autorizzazioni, all'autorità inquirente veniva consentito di richiedere all'impresa

di telecomunicazioni dati ai sensi dell'articolo 1111, paragrafo 2, della legge sulla comunicazione elettronica in merito a due numeri di abbonato e diversi identificatori internazionali apparecchiature mobili di H.K. relativi al periodo dal 1° gennaio al 2 febbraio 2015.

24. Da tale descrizione dei fatti del procedimento principale emerge che, nell'ambito del procedimento istruttorio, il pubblico ministero ha autorizzato l'autorità inquirente, ai sensi dell'articolo 901, paragrafo 2, del codice di procedura penale, a presentare richieste di fornitura di dati all'impresa di telecomunicazioni. Le autorizzazioni riguardanti i dati dei numeri di abbonato della persona indagata sono state rilasciate ai fini di un'indagine relativa a vari reati per una durata, rispettivamente, di un giorno, di circa un mese e di circa un anno.

25. H.K. ha proposto appello contro la sentenza del Viru Maakohus (Tribunale di primo grado di Viru) dinanzi alla Tartu Ringkonnakohus (Corte d'appello di Tartu, Estonia), che ha respinto tale appello con decisione del 17 novembre 2017. H.K. ha quindi proposto ricorso per cassazione dinanzi alla Riigikohus (Corte suprema), chiedendo l'annullamento delle decisioni di primo e secondo grado, la cessazione dei procedimenti penali nei propri confronti nonché il suo proscioglimento.

26. H.K. afferma che i verbali, nei quali sarebbero riportati i dati trasmessi dall'impresa di telecomunicazioni, non costituirebbero un mezzo di prova ammissibile e che la sua condanna sulla base dei medesimi sarebbe pertanto illegittima. Conformemente alla sentenza Tele2 Sverige e Watson e a., le norme di cui all'articolo 1111 della legge sulla comunicazione elettronica che prevedono l'obbligo per tali fornitori di servizi di conservare dati relativi alle comunicazioni nonché l'utilizzo di tali dati ai fini della sua condanna violerebbero l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8, 11 e 52, paragrafo 1, della Carta.

27. Secondo il giudice del rinvio, si pone quindi la questione se i verbali di cui trattasi, che l'autorità inquirente ha redatto sulla base di dati, contemplati all'articolo 1111, paragrafo 2, della legge sulla comunicazione elettronica, richiesti all'impresa di telecomunicazioni in virtù di un'autorizzazione del pubblico ministero, possano essere considerati mezzi di prova ammissibili.

28. I dati che i fornitori di servizi di comunicazione elettronica dovrebbero conservare per la durata di un anno includerebbero, inter alia, il numero del chiamante e del chiamato, il nome e l'indirizzo dell'abbonato, la data e l'orario di inizio e fine di una chiamata, il servizio di telefonia fissa o mobile utilizzato, l'identità utente mobile internazionale e l'identificatore internazionale apparecchiature mobili del chiamante e del chiamato nonché l'etichetta di ubicazione all'inizio della chiamata e i dati per identificare l'ubicazione geografica della cellula. Il giudice del rinvio rileva che si tratta di dati relativi all'avvenuta trasmissione di chiamate e messaggi per mezzo di un telefono fisso o mobile, nonché all'ubicazione dell'utilizzo dell'apparecchiatura terminale mobile, ma che tali dati non forniscono alcuna informazione quanto al contenuto delle comunicazioni stesse.

29. Come risulterebbe dalla sentenza Tele2 Sverige e Watson e a. nonché dalla sentenza del 2 ottobre 2018, Ministerio Fiscal (12), una normativa nazionale sulla conservazione di dati sul traffico

e di dati sull'ubicazione nonché sull'accesso a tali dati nel contesto di un procedimento penale, come l'articolo 1111, paragrafi 2 e 4, della legge sulla comunicazione elettronica e l'articolo 901, paragrafo 2, del codice di procedura penale, rientrerebbe nell'ambito di applicazione della direttiva 2002/58.

30. L'ammissibilità delle prove dipenderebbe dal rispetto delle disposizioni di diritto processuale relative alla loro raccolta. Pertanto, nel valutare se i verbali di cui trattasi nel procedimento principale siano ammissibili come mezzi di prova, occorrerebbe altresì acclarare in qual misura i dati su cui essi si fondano siano stati raccolti presso l'impresa di telecomunicazioni in conformità con l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8, 11 e 52, paragrafo 1, della Carta.

31. Alla luce delle sentenze Tele2 Sverige e Watson e a. (13) e Ministerio Fiscal (14), il giudice del rinvio si chiede se occorra interpretare l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8, 11 e 52, paragrafo 1, della Carta, nel senso che l'accesso di autorità nazionali a dati che consentano di rintracciare e identificare la fonte e la destinazione di una comunicazione telefonica a partire dal telefono fisso o mobile del sospettato, di determinarne la data, l'ora, la durata e la natura, di identificare le apparecchiature di comunicazione utilizzate, nonché di localizzare le apparecchiature di comunicazione mobile utilizzate, realizzi un'ingerenza nei diritti fondamentali sanciti dai suddetti articoli della Carta di gravità tale da dover limitare l'accesso stesso alla lotta contro la criminalità grave, indipendentemente dal periodo cui si riferiscono i dati conservati, ai quali tali autorità nazionali hanno chiesto di avere accesso.

32. In proposito, il giudice del rinvio considera che il periodo con riferimento al quale i dati di cui trattasi vengono richiesti costituisce una circostanza significativa ai fini della valutazione della gravità dell'ingerenza nei diritti fondamentali che l'accesso ai dati in questione costituirebbe. Sarebbe dunque possibile che tale ingerenza non debba essere considerata grave qualora i dati richiesti siano relativi soltanto ad un periodo molto breve, come un giorno. In tal caso, di regola, non sarebbe possibile trarre da tali dati conclusioni precise sulla vita privata della persona interessata, cosicché l'accesso delle autorità nazionali a detti dati potrebbe risultare giustificato da un obiettivo di accertamento e di perseguimento dei reati in generale.

33. Inoltre, il giudice del rinvio si chiede se l'accesso a dati come quelli che vengono in rilievo nel procedimento principale, alla luce degli insegnamenti che discendono dalla sentenza Ministerio Fiscal (15), possa essere giustificato dal medesimo obiettivo, qualora la quantità di dati ai quali le autorità hanno accesso sia limitata e, dunque, l'ingerenza nei diritti fondamentali di cui trattasi non sia grave. Riguardo alla quantità di dati, sarebbe essenziale tenere conto del tipo di dati (come quelli relativi alla destinazione della comunicazione o all'ubicazione dell'apparecchiatura) e della loro estensione temporale (ad esempio, un giorno, un mese oppure un anno). Secondo tale giudice, quanto più grave è il reato, tanto più gravi sarebbero le ingerenze nei diritti fondamentali ammesse nel procedimento, il che significa che maggiore sarebbe la quantità di dati ai quali le autorità nazionali possono avere accesso.

34. Infine, il giudice del rinvio si chiede se il pubblico ministero possa essere considerato un'autorità amministrativa «indipendente» ai sensi della sentenza Tele2 Sverige e Watson e a. (16). Esso rileva che, in Estonia, il pubblico ministero dirige il procedimento istruttorio, il cui obiettivo è, in particolare, la raccolta di prove. Il giudice del rinvio sottolinea inoltre che l'autorità inquirente e il pubblico ministero devono verificare gli elementi a carico e quelli a discarico del sospettato. Esso osserva infine che i poteri del pubblico ministero vengono esercitati, in nome del medesimo, da un procuratore, il quale agisce in modo indipendente, il che risulta dall'articolo 30, paragrafi 1 e 2, del codice di procedura penale e dagli articoli 1, paragrafi 1 e 11, nonché 2, paragrafo 2, della legge relativa al pubblico ministero.

35. In tale contesto, il giudice del rinvio sottolinea che i suoi dubbi riguardo all'indipendenza richiesta dal diritto dell'Unione sono principalmente dovuti al fatto che il pubblico ministero, in esito al procedimento istruttorio, formula l'imputazione nei confronti della persona interessata, qualora sia convinto che siano state raccolte tutte le prove necessarie e se ne ricorrono i presupposti. Detto giudice rileva che, in tal caso, è il pubblico ministero a rappresentare la pubblica accusa nel processo, ed egli è quindi anche parte del procedimento giudiziario. Il giudice del rinvio rileva inoltre che la Corte europea dei diritti dell'uomo ha già ammesso che, a determinate condizioni, possono essere autorizzati atti di sorveglianza in mancanza di un controllo preventivo da parte di un giudice, a condizione che un controllo giurisdizionale abbia luogo successivamente (17).

36. Ciò premesso, la Riigikohus (Corte suprema) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se l'articolo 15, paragrafo 1, della direttiva [2002/58] debba essere interpretato, alla luce degli articoli 7, 8, 11 e 52, paragrafo 1, della [Carta], nel senso che, in un procedimento penale, l'accesso di autorità nazionali a dati che consentano di rintracciare e identificare la fonte e la destinazione di una comunicazione telefonica a partire dal telefono fisso o mobile del sospettato, di determinarne la data, l'ora, la durata e la natura, di identificare le apparecchiature di comunicazione utilizzate, nonché di localizzare le apparecchiature di comunicazione mobile utilizzate, costituisca un'ingerenza nei diritti fondamentali sanciti dai suddetti articoli della Carta di gravità tale da dover limitare l'accesso stesso, quanto alla prevenzione, ricerca, accertamento e perseguimento dei reati, alla lotta contro la criminalità grave, indipendentemente dal periodo cui si riferiscono i dati conservati, ai quali le autorità nazionali hanno accesso.

2) Se l'articolo 15, paragrafo 1, della direttiva [2002/58] debba essere interpretato in base al principio di proporzionalità enunciato nella sentenza [Ministerio Fiscal], punti da 55 a 57, nel senso che, qualora la quantità dei dati menzionati nella prima questione, ai quali le autorità nazionali hanno accesso, non sia ingente (sia per il tipo di dati che per la loro estensione temporale), la conseguente ingerenza nei diritti fondamentali possa essere giustificata, in generale, dall'obiettivo di prevenzione, ricerca, accertamento e perseguimento dei reati e che i reati perseguiti mediante tale ingerenza debbano essere tanto più gravi quanto maggiore sia la quantità di dati cui le autorità nazionali hanno accesso.

3) Se il requisito indicato nel secondo punto del dispositivo della sentenza [Tele2 Sverige e Watson e a.], secondo cui l'accesso da parte delle autorità nazionali competenti ai dati dev'essere soggetto ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, implichi che l'articolo 15, paragrafo 1, della direttiva [2002/58] dev'essere interpretato nel senso che possa essere considerato quale autorità amministrativa indipendente il pubblico ministero che dirige il procedimento istruttorio e che, per legge, è tenuto ad agire in modo indipendente, restando soggetto soltanto alla legge e verificando, nell'ambito del procedimento istruttorio, sia gli elementi a carico sia quelli a discarico relativi all'indagato, ma che successivamente, nel procedimento giudiziario, rappresenti la pubblica accusa».

IV. Analisi

37. Con la prima e seconda questione pregiudiziale, il giudice del rinvio intende sapere, in sostanza, se l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8, 11 e 52, paragrafo 1, della Carta, debba essere interpretato nel senso che, tra i criteri che permettono di valutare la gravità dell'ingerenza nei diritti fondamentali costituita dall'accesso da parte delle autorità nazionali competenti a dati personali che i fornitori di servizi di comunicazione elettronica sono tenuti a conservare in forza di una normativa nazionale, rientrino le categorie di dati che vengono in rilievo nonché la durata del periodo con riferimento al quale l'accesso è richiesto.

38. Prima di rispondere a tale questione, formulerò due serie di osservazioni preliminari che mi consentiranno di rispondere, da un lato, agli argomenti addotti da taluni Stati membri per quanto concerne l'ambito di applicazione della direttiva 2002/58 e, dall'altro, al suggerimento della Commissione europea di esaminare, nel contesto del presente rinvio pregiudiziale, la compatibilità con il diritto dell'Unione della normativa estone, nella parte in cui impone ai fornitori di servizi di comunicazione elettronica di conservare varie categorie di dati personali creati nel contesto di tali servizi.

A. Osservazioni preliminari

1. Sull'ambito di applicazione della direttiva 2002/58

39. I governi irlandese, ungherese e polacco sollevano interrogativi riguardo all'ambito di applicazione della direttiva 2002/58.

40. Il governo irlandese sembra ritenere che una normativa nazionale relativa all'accesso da parte delle autorità competenti in materia penale a dati conservati esuli dall'ambito di applicazione della direttiva 2002/58, in forza dell'articolo 1, paragrafo 3, di quest'ultima.

41. Tale argomento dev'essere respinto ai sensi della giurisprudenza della Corte risultante dalle sentenze Tele2 Sverige e Watson e a. nonché Ministerio Fiscal.

42. Al riguardo, si deve rilevare che la Corte ha dichiarato che le misure legislative previste dall'articolo 15, paragrafo 1, della direttiva 2002/58 «rientrano nell'ambito di applicazione di tale direttiva, persino qualora rimandino ad attività proprie degli Stati o delle autorità statali, estranee ai settori di attività dei privati, e persino qualora le finalità che tali misure devono soddisfare coincidano sostanzialmente con le finalità perseguite dalle attività di cui all'articolo 1, paragrafo 3, della direttiva 2002/58» (18). Secondo la Corte, «[l]'articolo 15, paragrafo 1, di tale direttiva, infatti, presuppone necessariamente che le misure nazionali ivi indicate rientrino nell'ambito di applicazione della suddetta direttiva, poiché quest'ultima autorizza espressamente gli Stati membri ad adottarle solamente nel rispetto delle condizioni che essa prevede. Inoltre, le misure legislative contemplate dall'articolo 15, paragrafo 1, della direttiva 2002/58 disciplinano, per le finalità menzionate in tale disposizione, l'attività dei fornitori di servizi di comunicazione elettronica» (19).

43. La Corte ne ha tratto la conclusione che «il suddetto articolo 15, paragrafo 1, letto in combinato disposto con l'articolo 3 della direttiva 2002/58, deve essere interpretato nel senso che rientra nell'ambito di applicazione di tale direttiva non solo una misura legislativa che impone ai fornitori di servizi di comunicazione elettronica di conservare i dati relativi al traffico e i dati relativi all'ubicazione, ma anche una misura legislativa riguardante l'accesso delle autorità nazionali ai dati conservati da questi fornitori» (20).

44. Infatti, secondo la Corte, «la tutela della riservatezza delle comunicazioni elettroniche e dei dati relativi al traffico afferenti alle stesse, garantita dall'articolo 5, paragrafo 1, della direttiva 2002/58, si applica alle misure adottate da tutti i soggetti diversi dagli utenti, indipendentemente dal fatto che si tratti di persone o di enti privati oppure di enti statali. Come confermato dal considerando 21 di detta direttiva, quest'ultima mira a prevenire "l'accesso" non autorizzato alle comunicazioni, compreso "qualsiasi dato ad esse relativo", al fine di tutelare la riservatezza delle comunicazioni elettroniche» (21).

45. A tali argomenti, la Corte ha aggiunto che «misure legislative che impongano ai fornitori di servizi di comunicazione elettronica di conservare i dati personali o di accordare alle autorità nazionali competenti l'accesso a tali dati implicano necessariamente un trattamento, da parte dei fornitori suddetti, di questi dati (...). Misure di tal genere, nei limiti in cui disciplinano le attività dei fornitori menzionati, non possono pertanto essere considerate come attività proprie degli Stati, di cui all'articolo 1, paragrafo 3, della direttiva 2002/58» (22).

46. Analogamente a quanto dichiarato dalla Corte nella sentenza Ministerio Fiscal (23), dall'insieme di tali argomenti si deve dedurre che una domanda di accesso a dati personali conservati da fornitori di servizi di comunicazione elettronica, formulata nel contesto di un procedimento istruttorio penale, rientra nell'ambito di applicazione della direttiva 2002/58.

47. Peraltro, i governi ungherese e polacco adducono l'argomento secondo il quale il diritto dell'Unione non disciplina la questione dell'ammissibilità delle prove nei procedimenti penali.

48. Sebbene sia vero che, allo stato attuale della sua evoluzione, tale diritto non sancisce norme relative all'ammissibilità delle prove in un procedimento penale, il giudice del rinvio ha tuttavia chiaramente sottolineato in che modo l'interpretazione del diritto dell'Unione da lui richiesta si renda necessaria affinché possa pronunciarsi sull'ammissibilità delle prove. Quest'ultima, infatti, dipende dal rispetto delle condizioni e delle regole processuali relative alla raccolta di tali prove. Pertanto, in sede di valutazione dell'ammissibilità dei verbali di cui trattasi nel procedimento principale quali mezzi di prova, il giudice del rinvio deve chiedersi preliminarmente in che misura la raccolta dei dati presso l'impresa di telecomunicazioni, dati sui quali detti verbali si fondano, fosse conforme all'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8, 11 e 52, paragrafo 1, della Carta. Orbene, tale questione preliminare concerne un aspetto che, come ho precedentemente sottolineato, è disciplinato dal diritto dell'Unione. Relativamente a tale aspetto, le norme nazionali applicabili in materia di produzione della prova devono dunque rispettare gli obblighi derivanti dai diritti fondamentali garantiti dal diritto dell'Unione (24). Ciò premesso, l'argomento addotto dai governi ungherese e polacco, a mio parere, è inconferente.

2. Sulla conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione

49. Sebbene le questioni sollevate dal giudice del rinvio riguardino le condizioni di accesso ai dati, la Commissione invita la Corte a pronunciarsi, nel contesto del rinvio pregiudiziale in esame, anche sulla problematica relativa alla conservazione dei dati. In proposito, essa osserva, in sostanza, che l'accesso legittimo ai dati conservati esige che la normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica la conservazione dei dati creati nell'ambito di tali servizi soddisfi i requisiti sanciti dall'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce della Carta, o che i dati in questione siano stati conservati da tali fornitori di loro iniziativa, in particolare per scopi commerciali, conformemente alla medesima direttiva.

50. Per quanto attiene al procedimento principale, la Commissione osserva che i dati ai quali l'autorità inquirente ha avuto accesso sono stati conservati dai fornitori di servizi di comunicazione elettronica non già di loro iniziativa per scopi commerciali, bensì conformemente all'obbligo di conservazione loro imposto dall'articolo 1111 della legge sulla comunicazione elettronica. Essa rileva inoltre che H.K. contesta la legittimità delle norme nazionali relative tanto all'accesso ai dati quanto alla loro conservazione (25).

51. Ciò detto, rilevo che, come nel contesto del rinvio pregiudiziale che ha dato luogo alla sentenza Ministerio Fiscal (26), le questioni formulate dal giudice del rinvio nell'ambito della presente causa non mirano a stabilire se i dati personali di cui trattasi nel procedimento principale siano stati conservati dai fornitori di servizi di comunicazione elettronica in conformità con le condizioni di cui all'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8, 11 e 52, paragrafo 1, della Carta. Tali questioni vertono unicamente sulla compatibilità con le disposizioni in parola delle condizioni in base alle quali l'accesso da parte delle autorità nazionali inquirenti a simili

dati è autorizzato ai sensi della normativa estone. È per tale ragione che la discussione avviatasi dinanzi alla Corte ha riguardato quasi esclusivamente dette condizioni di accesso.

52. In ogni caso, il giudice del rinvio può basarsi sulla giurisprudenza risultante dalla sentenza Tele2 Sverige e Watson e a. qualora ritenga necessario, ai fini della risoluzione della controversia di cui al procedimento principale, statuire sulla compatibilità con il diritto dell'Unione dell'articolo 1111 della legge sulla comunicazione elettronica.

53. In proposito, mi limiterò a ricordare che, secondo la Corte, «l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, deve essere interpretato nel senso che esso osta ad una normativa nazionale la quale preveda, per finalità di lotta contro la criminalità, una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica» (27).

54. Compete al giudice del rinvio verificare, all'occorrenza, se la normativa estone imponga ai fornitori di servizi di comunicazione elettronica un obbligo di conservazione dei dati avente un simile carattere generalizzato e indifferenziato e trarne le conseguenze ai fini della risoluzione della controversia di cui al procedimento principale. Se la disciplina sulla conservazione dei dati predisposta dalla Repubblica d'Estonia dovesse essere considerata non conforme al diritto dell'Unione, in quanto sproporzionata alla luce dell'obiettivo perseguito, neppure l'accesso ai dati così conservati potrebbe essere giustificato da tale obiettivo.

55. Soltanto qualora tale obbligo di conservazione sia accompagnato da limiti appropriati, in particolare per quanto riguarda le categorie di dati che vengono in rilievo e la durata della conservazione, secondo una disciplina differenziata in funzione dell'obiettivo perseguito e strettamente necessaria al raggiungimento di quest'ultimo, esso potrà superare il controllo di proporzionalità.

56. Non mi soffermerò ulteriormente nel contesto delle presenti conclusioni sulla nozione di «conservazione limitata dei dati», esaminata dettagliatamente dall'avvocato generale Campos Sánchez-Bordona nelle conclusioni da lui presentate il 15 gennaio 2020 nell'ambito della causa Ordre des barreaux francophones et germanophone e a. (28).

B. Sull'accesso delle autorità nazionali competenti ai dati conservati

1. Insegnamenti tratti dalla sentenza Tele2 Sverige e Watson e a.

57. La Corte considera la problematica relativa all'accesso delle autorità nazionali competenti ai dati conservati «indipendentemente dall'ampiezza dell'obbligo di conservazione dei dati che

sarebbe imposto ai fornitori di servizi di comunicazione elettronica» e, in particolare, indipendentemente dal carattere generalizzato o mirato di una conservazione dei dati (29). Tale rilievo è correlato al fatto che la Corte considera la conservazione dei dati e l'accesso ad essi come due ingerenze distinte nei diritti fondamentali tutelati dalla Carta.

58. L'accesso ai dati conservati «deve rispondere in modo effettivo e rigoroso ad uno [degli] obiettivi» di cui all'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58. Inoltre deve esservi una concordanza tra la gravità dell'ingerenza e l'obiettivo perseguito. Se l'ingerenza è qualificata come «grave», essa può essere giustificata soltanto dalla lotta contro la criminalità grave (30).

59. Analogamente a ciò che si verifica per la conservazione dei dati, l'accesso a questi ultimi da parte delle autorità nazionali competenti può essere autorizzato soltanto entro i limiti dello stretto necessario (31). Inoltre, le misure legislative devono «prevedere (...) norme chiare e precise che indichino in quali circostanze e a quali condizioni i fornitori di servizi di comunicazione elettronica devono concedere alle autorità nazionali competenti l'accesso ai dati. Allo stesso modo, una misura di questa natura deve essere giuridicamente vincolante nell'ambito dell'ordinamento nazionale» (32). Più precisamente, le normative nazionali devono «prevedere anche le condizioni sostanziali e procedurali che disciplinano l'accesso delle autorità nazionali competenti ai dati conservati» (33).

60. Si può dedurre da quanto precede che «un accesso generale a tutti i dati conservati, indipendentemente da una qualche connessione, almeno indiretta, con la finalità perseguita, non può essere considerato limitato allo stretto necessario» (34).

61. Secondo la Corte, «la normativa nazionale in questione deve fondarsi su criteri oggettivi per definire le circostanze e le condizioni in presenza delle quali deve essere concesso alle autorità nazionali competenti l'accesso ai dati degli abbonati o degli utenti iscritti. A questo proposito, un accesso può, in linea di principio, essere consentito, in relazione con l'obiettivo della lotta contro la criminalità, soltanto per i dati di persone sospettate di progettare, di commettere o di aver commesso una violazione grave, o anche di essere implicate in una maniera o in un'altra in una violazione siffatta» (35).

62. In altri termini, la normativa nazionale che concede alle autorità nazionali competenti l'accesso ai dati conservati deve avere una portata sufficientemente delimitata al fine di impedire che un siffatto accesso possa riguardare un numero ingente di persone, o addirittura tutte le persone e tutti i mezzi di comunicazione elettronica nonché l'insieme dei dati conservati. Di conseguenza, la Corte ha esposto il criterio del collegamento tra le persone interessate e l'obiettivo perseguito.

63. Peraltro, la Corte ha stabilito le condizioni che qualsiasi accesso delle autorità nazionali competenti ai dati conservati deve soddisfare.

64. Anzitutto, tale accesso dev'essere «subordinato, in linea di principio, salvo casi di urgenza debitamente giustificati, ad un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente» (36). La decisione di tale giudice o di tale entità deve intervenire «a seguito di una richiesta motivata delle autorità suddette presentata, in particolare, nell'ambito di procedure di prevenzione, di accertamento o di esercizio dell'azione penale» (37).

65. Secondo la Corte, occorre inoltre che «le autorità nazionali competenti alle quali è stato consentito l'accesso ai dati conservati ne diano notizia alle persone interessate, nell'ambito delle procedure nazionali applicabili, a partire dal momento in cui tale comunicazione non è suscettibile di compromettere le indagini condotte dalle autorità summenzionate» (38).

66. Infine, gli Stati membri devono adottare norme aventi ad oggetto la sicurezza e la protezione dei dati conservati da parte dei fornitori di servizi di comunicazione elettronica, al fine di evitare gli abusi nonché qualsiasi accesso illecito ai dati (39).

2. Insegnamenti tratti dalla sentenza Ministerio Fiscal

67. In tale causa, la Corte era chiamata a pronunciarsi sulla questione della compatibilità con l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7 e 8 della Carta, di una normativa nazionale che preveda l'accesso da parte delle autorità nazionali competenti, come la polizia giudiziaria, a dati relativi all'identità civile dei titolari di alcune schede SIM.

68. Nella sua sentenza, la Corte ha rilevato che, per quanto riguarda l'obiettivo di prevenzione, ricerca, accertamento e perseguimento dei reati, la formulazione dell'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58 non limita tale obiettivo alla lotta contro i soli reati gravi, ma si riferisce ai «reati» in generale (40).

69. Il ragionamento svolto dalla Corte chiarisce la circostanza che, per quanto attiene all'accesso ai dati da parte delle autorità nazionali competenti, deve sussistere una corrispondenza tra la gravità dell'ingerenza e la gravità degli illeciti di cui trattasi.

70. Quindi, la Corte ricorda, riferendosi al punto 99 della sua sentenza Tele2 Sverige e Watson e a., che essa ha certo affermato che, «in materia di prevenzione, ricerca, accertamento e perseguimento dei reati, soltanto la lotta contro la criminalità grave è idonea a giustificare un accesso delle autorità pubbliche a dati personali conservati dai fornitori di servizi di comunicazione che, considerati nel loro insieme, consentono di trarre conclusioni precise sulla vita privata delle persone i cui dati sono oggetto di attenzione» (41).

71. Tuttavia, la Corte precisa che essa ha «motivato tale interpretazione affermando che l'obiettivo perseguito da una normativa che disciplina tale accesso deve essere adeguat[o] alla gravità dell'ingerenza nei diritti fondamentali in questione che tale operazione determina» (42).

72. «In conformità al principio di proporzionalità, infatti, una grave ingerenza può essere giustificata, in materia di prevenzione, ricerca, accertamento e perseguimento di un reato, solo da un obiettivo di lotta contro la criminalità che deve essere qualificata come "grave"» (43).

73. Al contrario, «qualora l'ingerenza che comporta tale accesso non sia grave, detto accesso può essere giustificato da un obiettivo di prevenzione, ricerca, accertamento e perseguimento di un "reato" in generale» (44).

74. Tali considerazioni imponevano dunque di chiedersi se, alla luce delle circostanze del caso di specie, l'ingerenza nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta che un accesso della polizia giudiziaria ai dati oggetto del procedimento principale avrebbe comportato dovesse o meno essere considerata «grave».

75. Orbene, diversamente da quanto avvenuto nella sentenza Tele2 Sverige e Watson e a., l'ingerenza nei diritti tutelati agli articoli 7 e 8 della Carta, costituita dall'accesso ai dati di cui si trattava, non è stata qualificata come «grave» dalla Corte (45). Infatti, la domanda di accesso aveva «il solo scopo di identificare i titolari delle carte SIM attivate, per un periodo di dodici giorni, con il codice [relativo all'identificatore internazionale apparecchiature mobili] del telefono cellulare rubato» (46). Si trattava dell'accesso «ai soli numeri di telefono corrispondenti a tali carte SIM e ai dati relativi all'identità civile dei titolari di dette carte, quali il loro cognome e, se del caso, indirizzo. Al contrario, tali dati non riguarda[vano] (...) le comunicazioni effettuate con il telefono cellulare rubato o l'ubicazione di quest'ultimo» (47).

76. La Corte ne ha dedotto che «i dati oggetto della domanda di accesso di cui al procedimento principale consentono unicamente di collegare, nel corso di un determinato periodo, la o le carte SIM attivate con il telefono cellulare rubato con l'identità civile dei titolari di tali carte SIM. Senza una verifica incrociata dei dati relativi alle comunicazioni effettuate con tali schede SIM e dei dati relativi all'ubicazione, questi dati non permettono di conoscere né la data, né l'ora, né la durata, né i destinatari delle comunicazioni effettuate con la o le carte SIM in questione, né i luoghi in cui dette comunicazioni sono avvenute o la frequenza di esse con talune persone nel corso di un determinato periodo. Questi dati non permettono quindi di trarre conclusioni precise sulla vita privata delle persone i cui dati sono oggetto di attenzione» (48).

77. Una volta esclusa la qualifica come «ingerenza grave», la Corte ha potuto considerare che l'obiettivo di prevenzione, ricerca, accertamento e perseguimento di reati in generale, anche non gravi, poteva essere addotto per giustificare l'ingerenza in questione (49).

78. È alla luce di tale giurisprudenza che il giudice del rinvio solleva la prima e la seconda questione pregiudiziale, allo scopo di valutare la gravità dell'ingerenza costituita dall'accesso ai dati nel contesto del procedimento penale di cui trattasi in via principale. Più precisamente, esso intende sapere se le categorie di dati che vengono in rilievo nonché la durata del periodo con riferimento al quale l'accesso a tali dati è richiesto costituiscano, in tale prospettiva, criteri rilevanti.

3. Sui criteri che permettono di valutare la gravità dell'ingerenza

79. Come risulta dalla giurisprudenza della Corte, l'ingerenza può essere qualificata tanto più «grave» quanto più numerose sono le categorie di dati a cui si richiede di accedere.

80. Ciò premesso, la prima e la seconda questione che solleva il giudice del rinvio condurranno la Corte a precisare se, oltre alle categorie di dati che vengono in rilievo, anche l'estensione del periodo interessato da tale accesso svolga un ruolo in sede di determinazione della gravità dell'ingerenza.

81. A mio avviso, la risposta dovrebbe essere affermativa. Rilevo del resto che, nella sentenza Ministerio Fiscal, la Corte, nell'ambito della propria valutazione, ha tenuto conto anche della durata del periodo interessato dall'accesso, ossia dodici giorni nel caso di specie (50).

82. Combinando la natura dei dati considerati e la durata del periodo oggetto dell'accesso è possibile valutare la gravità dell'ingerenza. Questi due aspetti consentono, infatti, di verificare se il criterio decisivo per la gravità dell'ingerenza sia soddisfatto, ossia se l'accesso ai dati di cui trattasi possa permettere alle autorità nazionali competenti di trarre conclusioni precise riguardo alla vita privata delle persone i cui dati sono interessati da tale accesso. Orbene, per poter delineare il preciso ritratto di una persona, è necessario non soltanto che l'accesso riguardi più categorie di dati, come i dati identificativi, relativi al traffico e i dati relativi all'ubicazione, ma anche che tale accesso abbia ad oggetto un periodo abbastanza lungo da poter rivelare con sufficiente precisione gli aspetti principali della vita di una persona.

83. Al pari del numero di categorie interessate, la durata del periodo per cui sono richiesti dati conformemente a un'autorizzazione di accesso costituisce dunque un elemento essenziale ai fini della valutazione della gravità dell'ingerenza nei diritti fondamentali delle persone interessate. Come afferma la Commissione, deve parimenti essere preso in considerazione il cumulo di varie domande di accesso relative a una sola persona, anche se esse concernono periodi brevi.

84. Come risulta dalla domanda di pronuncia pregiudiziale, i dati ai quali l'autorità inquirente ha avuto accesso sono quelli contemplati all'articolo 1111, paragrafo 2, della legge sulla comunicazione elettronica. Tali dati consentono di rintracciare e identificare la fonte e la destinazione di una sessione di comunicazione telefonica a partire dal telefono fisso o mobile di una persona, di determinarne la data, l'ora, la durata e la natura, di identificare le apparecchiature di comunicazione

utilizzate, nonché di localizzare le apparecchiature di comunicazione mobile utilizzate. Tali dati sono stati trasmessi all'autorità inquirente per periodi di un giorno, di un mese e di quasi un anno.

85. La valutazione del grado dell'ingerenza nei diritti fondamentali derivante dall'accesso delle autorità nazionali competenti ai dati personali conservati risulta da un esame concreto delle circostanze proprie di ciascun caso di specie. In ciascuna ipotesi, compete al giudice del rinvio valutare se i dati ai quali è stato autorizzato l'accesso fossero tali da permettere, in base alla loro natura e alla durata del periodo oggetto di detto accesso, di trarre conclusioni precise sulla vita privata delle persone interessate.

86. Se così è, l'ingerenza dovrebbe essere qualificata come «grave» ai sensi della giurisprudenza della Corte e, dunque, potrebbe essere giustificata, in materia di prevenzione, ricerca, accertamento e perseguimento di un reato, solo da un obiettivo di lotta contro la criminalità che dovrebbe essere parimenti qualificata come «grave» (51).

4. Sulla corrispondenza tra la gravità dell'ingerenza e l'obiettivo perseguito

87. Dalla giurisprudenza della Corte risulta che un'ingerenza nei diritti fondamentali qualificata come «grave» implica la necessità di una giustificazione rafforzata.

88. Per quanto concerne la gravità dei presunti reati in relazione ai quali è stato concesso l'accesso ai dati, la Commissione osserva che la normativa nazionale che viene in rilievo nel procedimento principale autorizza segnatamente l'accesso per contrastare i reati in generale (52).

89. Compete al giudice del rinvio verificare, in funzione delle circostanze del caso di specie, se l'accesso a dati come quelli di cui trattasi nel procedimento principale risponda in modo effettivo e rigoroso a uno degli obiettivi di cui all'articolo 15, paragrafo 1, della direttiva 2002/58. In proposito, si deve ricordare che tale disposizione non limita l'obiettivo di prevenzione, ricerca, accertamento e perseguimento dei reati alla lotta contro i soli reati gravi, ma si riferisce ai «reati» in generale (53).

90. Il giudice del rinvio, qualora pervenga alla conclusione che l'ingerenza dev'essere qualificata come «grave», è tenuto a valutare se anche il reato in questione possa essere qualificato come «grave» secondo il diritto penale nazionale.

91. In proposito, ritengo che la definizione di ciò che può essere qualificato come «reato grave» debba essere lasciata alla valutazione discrezionale degli Stati membri.

92. Infatti, a seconda dei sistemi giuridici nazionali, lo stesso reato può essere sanzionato più o meno severamente. La definizione delle circostanze aggravanti può parimenti variare a seconda degli Stati membri.

93. Come correttamente rilevato dal governo estone, per stabilire la gravità dei reati, la pena applicabile non è l'unico criterio. Occorre altresì prendere in considerazione la natura dei reati, il danno che causano alla società, il pregiudizio che arrecano ai beni giuridici e i loro effetti complessivi sull'ordinamento giuridico nazionale nonché sui valori di una società democratica. Anche il contesto storico, economico e sociale specifico di ciascuno Stato membro svolge un ruolo in proposito. Peraltro, con riferimento alle circostanze aggravanti, occorre chiedersi se i reati siano stati commessi, ad esempio, in maniera reiterata oppure nei confronti di un gruppo di persone vulnerabili.

94. Al fine di valutare la proporzionalità dell'accesso, si deve inoltre tener conto del fatto che, conformemente all'articolo 901, paragrafo 3, del codice di procedura penale, «i dati possono essere richiesti soltanto laddove ciò sia indispensabile al fine di raggiungere lo scopo del procedimento penale». Come afferma il governo estone, il criterio dell'assoluta necessità (54) obbliga tanto gli inquirenti quanto i soggetti preposti al rilascio dell'autorizzazione a considerare e a valutare quali dati siano necessari per il buon esito del procedimento penale e senza i quali non sarebbe possibile, nel contesto di un determinato procedimento, consentire di far emergere la verità o catturare un presunto delinquente o criminale.

95. Aggiungo che, come correttamente sottolineato dal governo francese, il grado di gravità di un reato o anche la sua esatta qualificazione giuridica non possono essere sempre determinati con precisione qualora l'autorizzazione di accesso a dati conservati intervenga in una fase precoce dell'indagine, cosicché in tale fase potrebbe sembrare prematuro far rientrare detto reato nella categoria dei reati gravi o in quella dei reati in generale. Tale incertezza, inerente alle indagini penali il cui stesso scopo è contribuire alla manifestazione della verità, dev'essere presa in considerazione dal giudice del rinvio nell'ambito della sua valutazione relativa al carattere proporzionato dell'accesso.

96. Ciò premesso, l'incertezza che può quindi sussistere all'inizio dell'indagine penale riguardo a tali aspetti non può far venir meno il requisito secondo cui ciascuna domanda di accesso dev'essere motivata dalla necessità di ricercare prove relative a una specifica condotta delittuosa, sulla base di un sospetto avvalorato da elementi obiettivi. Pertanto, una domanda di accesso non può avere per scopo l'esame, nell'arco di un dato periodo, di tutti i fatti e gesti di una persona, in vista della ricerca di eventuali reati. Peraltro, se nel corso dell'indagine emergono nuovi fatti, l'accesso ai dati al fine di provare questi ultimi dovrà essere oggetto di una nuova autorizzazione di accesso.

97. Tenuto conto delle precedenti considerazioni, suggerisco alla Corte di dichiarare che l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8, 11 e 52, paragrafo 1, della Carta, dev'essere interpretato nel senso che, tra i criteri che permettono di valutare la gravità dell'ingerenza nei diritti fondamentali costituita dall'accesso da parte delle autorità nazionali

competenti a dati personali che i fornitori di servizi di comunicazione elettronica sono tenuti a conservare in forza di una normativa nazionale, rientrano le categorie di dati che vengono in rilievo nonché la durata del periodo con riferimento al quale tale accesso è richiesto. Compete al giudice del rinvio valutare, in funzione della gravità dell'ingerenza, se detto accesso fosse strettamente necessario in vista del raggiungimento dell'obiettivo di garantire la prevenzione, la ricerca, l'accertamento e il perseguimento dei reati.

C. Controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente

98. Allo scopo di garantire che l'accesso da parte delle autorità nazionali competenti ai dati conservati sia limitato allo stretto necessario ai fini del raggiungimento dell'obiettivo perseguito, la Corte ha considerato che è essenziale che tale accesso «sia subordinato, in linea di principio, salvo casi di urgenza debitamente giustificati, ad un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente, e che la decisione di tale giudice o di tale entità intervenga a seguito di una richiesta motivata delle autorità suddette presentata, in particolare, nell'ambito di procedure di prevenzione, di accertamento o di esercizio dell'azione penale» (55).

99. Con la terza questione pregiudiziale, il giudice del rinvio invita la Corte a precisare i criteri che un'autorità amministrativa deve soddisfare per poter essere considerata «indipendente», ai sensi della sentenza Tele2 Sverige e Watson e a. Più precisamente, il giudice del rinvio si chiede se il pubblico ministero possa essere considerato quale autorità amministrativa indipendente, tenuto conto del fatto che dirige il procedimento istruttorio e rappresenta la pubblica accusa nel corso del processo.

100. Al fine di rispondere a tale interrogativo, mi sembra utile prendere in considerazione due aspetti della giurisprudenza della Corte, ossia, da un lato, la giurisprudenza relativa all'indipendenza delle autorità nazionali di controllo della protezione dei dati personali e, dall'altro, la giurisprudenza relativa all'indipendenza dell'autorità giudiziaria emittente nel contesto del mandato di arresto europeo.

101. Secondo la Corte, l'indipendenza costituisce una caratteristica essenziale, affermata in particolare all'articolo 8, paragrafo 3, della Carta, delle autorità incaricate di controllare l'osservanza delle norme dell'Unione relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, diretta ad assicurare che tale controllo sia efficace e affidabile e a rafforzare la protezione delle persone interessate dalle decisioni di tali autorità (56).

102. La Corte ha già statuito, a proposito dell'articolo 28, paragrafo 1, secondo comma, della direttiva 95/46, che «le autorità di controllo competenti per la vigilanza del trattamento dei dati personali devono godere di un'indipendenza che consenta loro di svolgere le proprie funzioni senza subire influenze esterne. Tale indipendenza esclude in particolare qualsiasi imposizione e ogni altra influenza esterna di qualunque forma, sia diretta che indiretta, che possano orientare le loro decisioni e che potrebbero quindi rimettere in discussione lo svolgimento, da parte di dette autorità,

del loro compito, consistente nello stabilire un giusto equilibrio tra la protezione del diritto alla vita privata e la libera circolazione dei dati personali» (57).

103. La Corte ha inoltre posto l'accento sulla necessità che, alla luce del loro ruolo di custodi della vita privata, tali autorità di controllo siano «al di sopra di qualsivoglia sospetto di parzialità» (58).

104. Dato che la terza questione sollevata dal giudice del rinvio riguarda il pubblico ministero, è altresì pertinente la considerazione dei criteri formulati dalla Corte nella sua giurisprudenza relativa all'indipendenza dell'autorità giudiziaria emittente nel contesto del mandato di arresto europeo. Così, secondo la Corte, il controllo effettuato al momento dell'adozione di un mandato d'arresto «deve essere esercitato in maniera obiettiva, tenendo conto di tutti gli elementi a carico e a discarico, nonché in modo indipendente, il che presuppone che vi siano regole statutarie e organizzative idonee ad escludere qualsiasi rischio che l'adozione di una decisione di emettere un siffatto mandato d'arresto sia sottoposta a istruzioni esterne, segnatamente da parte del potere esecutivo» (59). Si deve tuttavia ricordare che la valutazione concreta da parte della Corte, in ciascun caso, della questione se il pubblico ministero soddisfi o meno i summenzionati criteri (60) è effettuata nello specifico contesto dell'emissione di un mandato di arresto europeo e, dunque, non è automaticamente trasponibile ad altri settori, come quello relativo alla protezione dei dati personali.

105. Ciò precisato, i due aspetti della giurisprudenza della Corte convergono sottolineando, in ciascuno dei settori di cui trattasi, che l'autorità nazionale competente a verificare il rispetto delle norme del diritto dell'Unione deve avere carattere indipendente, il che si traduce in due presupposti (61). Da un lato, tale autorità non deve essere soggetta a istruzioni o pressioni esterne che possano influenzarne le decisioni. D'altro lato, detta autorità, in virtù del proprio status e dei compiti che le sono conferiti, deve soddisfare un requisito di obiettività nell'ambito del controllo da essa effettuato, ossia deve offrire garanzie di imparzialità. Più specificamente, la valutazione da parte di un'autorità amministrativa della proporzionalità dell'accesso ai dati conservati richiede che essa sia in condizione di realizzare il giusto equilibrio tra gli interessi connessi all'efficacia dell'indagine nel contesto della lotta contro la criminalità e quelli correlati alla protezione dei dati personali delle persone toccate dall'accesso. Con riferimento a quest'ultimo aspetto, il requisito di imparzialità è pertanto inerente alla nozione di «autorità amministrativa indipendente» evidenziata dalla Corte nella sentenza Tele2 Sverige e Watson e a.

106. Occorre verificare se il pubblico ministero, tenuto conto dei differenti compiti attribuitigli dalla normativa estone, rispetti tale criterio di indipendenza, nelle sue due dimensioni, quando è chiamato a controllare il carattere strettamente necessario dell'accesso ai dati. Quindi, la nozione di «indipendenza» che deve caratterizzare l'autorità amministrativa incaricata di un siffatto controllo assume una dimensione funzionale, nel senso che è alla luce dello specifico oggetto di tale controllo che occorre valutare se tale autorità sia in grado di agire in assenza di interventi e pressioni esterne che possano influenzarne le decisioni, nonché nel rispetto dell'obiettività e della rigorosa applicazione della norma giuridica. In sintesi, la nozione di «autorità amministrativa indipendente» ai sensi della sentenza Tele2 Sverige e Watson e a. è destinata a garantire l'obiettività, l'affidabilità e l'efficacia del controllo in parola.

107. Ciò implica di valutare se la normativa estone che precisa lo status ed i compiti del pubblico ministero possa ingenerare dubbi legittimi, nelle persone interessate, riguardo all'impermeabilità dei procuratori rispetto ad elementi esterni e alla loro neutralità con riferimento agli interessi che si contrappongono, allorché sono chiamati ad assicurare il controllo preventivo sulla proporzionalità dell'accesso ai dati.

108. Il pubblico ministero gioca un ruolo essenziale nello svolgimento del procedimento penale, in quanto dirige il procedimento istruttorio e, in particolare, dispone della competenza a esercitare un'azione penale nei confronti di una persona sospettata di aver commesso un reato affinché quest'ultima compaia dinanzi a un giudice. In tal senso, deve essere considerato un'autorità che partecipa all'amministrazione della giustizia penale (62).

109. Come affermato dalla Corte a proposito della Procura della Repubblica (Italia), e secondo una formula che ritengo sia trasponibile al contesto della presente causa, il procuratore ha «il compito (...) non già di dirimere con assoluta indipendenza una controversia, ma di sottoporla eventualmente, in quanto parte che esercita l'azione penale nel processo, al giudizio dell'organo giurisdizionale competente» (63).

110. Sebbene il pubblico ministero presenti pertanto, per quanto attiene al suo status, alla sua organizzazione e ai suoi compiti, tratti particolari che lo distinguono da un giudice e che giustificano che sia qualificato come «autorità che partecipa all'amministrazione della giustizia penale negli Stati membri», resta nondimeno il fatto che, da un punto di vista funzionale, quando il diritto nazionale prevede che l'autorità che esercita il controllo preventivo sulla proporzionalità dell'accesso imposto dalla sentenza Tele2 Sverige e Watson e a. sia il pubblico ministero, quest'ultimo, con riferimento a tale aspetto, deve mostrare un grado di indipendenza analogo a quello di un giudice. Infatti, l'esercizio di tale funzione da parte di un'autorità amministrativa anziché da parte di un giudice non deve incidere sull'obiettività, sull'affidabilità e sull'efficacia di tale controllo.

111. In proposito, va ricordato che, conformemente all'articolo 901, paragrafo 2, del codice di procedura penale, l'autorità inquirente, con l'autorizzazione del pubblico ministero nel corso del procedimento istruttorio o con l'autorizzazione del tribunale nel corso del processo dinanzi a quest'ultimo, può chiedere a un'impresa di comunicazioni elettroniche di fornire i dati elencati all'articolo 1111, paragrafi 2 e 3, della legge sulla comunicazione elettronica.

112. Peraltro, dalla normativa estone risulta che il pubblico ministero, nell'ambito di un procedimento penale, dirige il procedimento istruttorio, il cui obiettivo è la raccolta di mezzi di prova e la predisposizione delle altre condizioni necessarie allo svolgimento di un processo. Inoltre, nel corso del procedimento istruttorio, l'autorità inquirente e il pubblico ministero verificano gli elementi a carico e quelli a discarico raccolti nei confronti del sospettato o dell'indagato. Qualora il pubblico ministero si convinca che siano state raccolte tutte le prove necessarie e se ne ricorrono i

presupposti, egli formula l'imputazione nei confronti della persona e, in tal caso, rappresenta la pubblica accusa in giudizio.

113. Il giudice del rinvio osserva altresì che sebbene, nel contesto del procedimento penale, il pubblico ministero, per le misure che comportano le ingerenze più gravi nei diritti fondamentali, debba ottenere l'autorizzazione di un giudice istruttore (ad esempio, per la maggior parte delle misure di sorveglianza e per la custodia), rientra tra i poteri del pubblico ministero anche la decisione su alcune misure procedurali che presentano un'intensa ingerenza in vari diritti fondamentali (64).

114. I dubbi espressi dal giudice del rinvio riguardo alla qualificazione del pubblico ministero come «autorità amministrativa indipendente» ai sensi della sentenza Tele2 Sverige e Watson e a. sono principalmente dovuti al fatto che qualora, successivamente al procedimento istruttorio, il pubblico ministero si convinca che siano state raccolte tutte le prove necessarie per l'avvio del procedimento penale e se ne ricorrono i presupposti, gli spetta formulare l'imputazione contro la persona interessata. In tal caso, il pubblico ministero rappresenta la pubblica accusa nel processo ed è quindi anche parte del procedimento giudiziario. Pertanto, la qualificazione del pubblico ministero come «autorità amministrativa indipendente» ai sensi della sentenza Tele2 Sverige e Watson e a. è messa in dubbio dal giudice del rinvio principalmente a causa della sua qualità di parte accusatrice.

115. Espressi in tal modo, i dubbi del giudice del rinvio riguardano dunque più specificamente l'imparzialità del pubblico ministero nel contesto del controllo sulla proporzionalità dell'accesso ai dati da parte dei servizi inquirenti che egli è tenuto a effettuare prima di autorizzare un simile accesso.

116. Prima di affrontare tale aspetto relativo all'imparzialità, rilevo che l'articolo 1, paragrafo 11, della legge relativa al pubblico ministero stabilisce che quest'ultimo, «nell'esercizio delle funzioni assegnategli dalla legge, è indipendente». Inoltre, ai sensi dell'articolo 2, paragrafo 2, di tale legge, «[i]l procuratore, nell'esercizio delle proprie funzioni, è indipendente e agisce esclusivamente secondo la legge e secondo il proprio convincimento» (65).

117. In proposito, il governo estone dichiara che, sebbene il pubblico ministero sia un'autorità che dipende dal Ministero della Giustizia, la normativa estone nega tuttavia a quest'ultimo qualsiasi possibilità di formulare una valutazione su un procedimento specifico o di intervenire in un procedimento penale in corso. Tale governo precisa che ignorare l'indipendenza del pubblico ministero costituirebbe un illecito sanzionabile.

118. Sebbene, pertanto, non si possa dubitare dell'indipendenza del pubblico ministero nel contesto dei compiti affidatigli ai sensi della normativa estone, mi sembra tuttavia che quest'ultima possa suscitare dubbi legittimi in ordine all'idoneità del pubblico ministero ad esercitare un controllo preventivo neutro e obiettivo sul carattere proporzionato dell'accesso ai dati qualora, nell'ambito di un dato caso, possa essere chiamato a svolgere al contempo i compiti consistenti nel dirigere

l’indagine penale, nel decidere sull’esercizio dell’azione penale e nel rappresentare la pubblica accusa in giudizio.

119. Vero è che vari elementi contenuti nella normativa estone costituiscono garanzie che, nel contesto delle funzioni che esercita, il pubblico ministero agisca nel rispetto del requisito di imparzialità.

120. In tal senso, in forza dell’articolo 211, paragrafo 2, del codice di procedura penale, il pubblico ministero è tenuto a verificare gli elementi a carico e quelli a discarico raccolti nei confronti del sospettato o dell’indagato.

121. Peraltro, come risulta dall’articolo 1, paragrafo 1, della legge relativa al pubblico ministero, quest’ultimo è tenuto ad assicurare la legittimità del procedimento istruttorio penale che ha il compito di dirigere. Inoltre, conformemente agli articoli 1, paragrafo 11, e 2, paragrafo 2, della medesima legge, il pubblico ministero deve esercitare i propri compiti nel rispetto delle leggi. Ciò presuppone che, quando dirige il procedimento istruttorio penale, il pubblico ministero debba perseguire non soltanto l’obiettivo di assicurare l’efficacia di quest’ultimo, ma anche di garantire che tale procedimento non si svolga arrecando un pregiudizio sproporzionato al diritto alla vita privata delle persone interessate. Infatti, si può ritenere che l’autorizzazione di accesso ai dati conservati sia parte integrante del compito più generale del pubblico ministero, consistente nel controllo sulla legittimità degli strumenti messi in atto dai servizi inquirenti, in particolare sulla proporzionalità degli atti di indagine alla luce della natura e della gravità dei fatti.

122. Pertanto, si potrebbe sostenere che è proprio perché dirige il procedimento istruttorio che il pubblico ministero è in grado di valutare se, in considerazione delle specificità di ciascun caso, un accesso a dati conservati dagli operatori di telecomunicazione sia strettamente necessario, in mancanza di elementi di prova alternativi, per far avanzare l’indagine relativa ad un presunto reato.

123. Resta nondimeno il fatto che, dal punto di vista delle persone interessate dalla domanda di accesso ai dati, la circostanza che l’autorità amministrativa che è tenuta a verificare se tale accesso sia strettamente necessario nel contesto dell’indagine sia, al contempo, quella che può perseguirle e poi rappresentare la pubblica accusa nel corso di un eventuale successivo processo, a mio avviso, può indebolire le garanzie di imparzialità previste dalla normativa estone. Da questo punto di vista, può sussistere un potenziale conflitto fra tali compiti del pubblico ministero, da un lato, e la condizione di neutralità e di obiettività del controllo preventivo sulla proporzionalità dell’accesso ai dati, dall’altro.

124. Infatti, nell’ambito dei propri compiti, il pubblico ministero è tenuto a raccogliere le prove, a valutarne la rilevanza e a trarre conclusioni riguardo alla colpevolezza dell’interessato. Spetta a tale autorità statale presentare e corroborare il fascicolo accusatorio nel contesto della pubblica accusa che è chiamata a rappresentare in giudizio, essendo dunque parte del procedimento. A causa di detti compiti, il pubblico ministero è tenuto ad assolvere un onere probatorio, il quale, agli occhi dei

sospettati di aver commesso un reato, può apparire come incompatibile con l'idoneità della medesima autorità a effettuare, in maniera neutra e obiettiva, un controllo preventivo sulla proporzionalità dell'accesso ai dati.

125. Come rilevato dalla Commissione, potrebbe esservi il rischio che, a causa del cumulo dei compiti a cui è tenuto, vi sia nelle persone coinvolte la percezione che il pubblico ministero abbia un interesse a concedere un ampio accesso ai loro dati, siano essi a carico o a discarico. Inoltre, le persone sospettate di aver commesso un reato possono nutrire dubbi legittimi sull'imparzialità del pubblico ministero allorché questi autorizza l'accesso ai loro dati, in quanto egli può agire contro di loro nella fase successiva, a titolo di parte accusatrice. Orbene, ritengo che il requisito di imparzialità dell'autorità amministrativa incaricata di effettuare il controllo preventivo richiesto dalla sentenza Tele2 Sverige e Watson e a. presupponga una certa distanza e una neutralità rispetto agli interessi che possono contrapporsi nel contesto del procedimento istruttorio, ossia, da un lato, l'efficacia di quest'ultima e, dall'altro, la protezione dei dati personali delle persone coinvolte. Secondo la Commissione, la situazione potrebbe essere differente se l'organizzazione amministrativa interna del pubblico ministero fosse tale da far sì che il procuratore che deve pronunciarsi sulla domanda di accesso non svolga alcun ruolo nel procedimento istruttorio e nelle fasi successive del procedimento penale, inclusa la pubblica accusa.

126. Considerato che, come confermato all'udienza, nella Repubblica d'Estonia la procura è organizzata gerarchicamente, non sono certo che tale suggerimento della Commissione possa rimediare agli inconvenienti derivanti dal cumulo dei compiti che la normativa estone pone a carico del pubblico ministero. In ogni caso, ciò non fa venir meno la rilevanza dell'idea sottesa a tale suggerimento, ossia che il controllo preventivo sulla proporzionalità dell'accesso ai dati debba essere effettuato da un'autorità amministrativa che, da un lato, non sia direttamente coinvolta nella direzione dell'indagine penale in oggetto e, d'altro lato, si trovi in una posizione di neutralità nei confronti delle parti del procedimento penale. Una simile autorità, svincolata dagli interessi connessi all'indagine e alla pubblica accusa nel procedimento in oggetto, non potrebbe essere tacciata di privilegiare gli interessi dell'indagine a scapito di quelli relativi alla protezione dei dati delle persone coinvolte. Detta autorità sarebbe allora in condizione di adottare, in una situazione di completa imparzialità, una decisione che limiti l'accesso ai dati conservati a quanto strettamente necessario ai fini del raggiungimento dell'obiettivo perseguito, conformemente a quanto richiesto dall'articolo 15, paragrafo 1, della direttiva 2002/58, come interpretato dalla Corte nelle sentenze dell'8 aprile 2014, Digital Rights Ireland e a. (66), e Tele2 Sverige e Watson e a. Al contempo, sono perfettamente consapevole che l'istituzione di un punto di vista esterno rispetto agli interessi connessi al procedimento in oggetto non debba avvenire a costo di una riduzione dell'efficacia della ricerca, del perseguimento e della repressione dei reati.

127. Al fine di rispettare l'autonomia procedurale degli Stati membri, la Corte non dovrebbe intromettersi ulteriormente nell'organizzazione generale dell'amministrazione della giustizia negli Stati membri e neppure nell'organizzazione interna delle procure. Compete agli Stati membri predisporre gli strumenti idonei a garantire che il controllo preliminare all'accesso ai dati conservati assicuri un giusto equilibrio tra gli interessi connessi all'efficacia dell'indagine penale e il diritto alla protezione dei dati delle persone interessate da tale accesso.

128. Terminerò precisando che, a mio avviso, l'assenza di un controllo preventivo effettuato da un'autorità amministrativa «indipendente» ai sensi della sentenza Tele2 Sverige e Watson e a. non può essere compensata dall'esistenza di un controllo giurisdizionale effettuabile dopo che l'accesso è stato autorizzato (67). In caso contrario, la condizione relativa al carattere preventivo del controllo perderebbe la sua ragion d'essere, consistente nell'impedire che venga autorizzato un accesso ai dati conservati che sia sproporzionato rispetto all'obiettivo consistente nel ricercare, perseguire e reprimere i reati.

129. Alla luce delle precedenti considerazioni, suggerisco alla Corte di rispondere alla terza questione pregiudiziale dichiarando che l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alle luce degli articoli 7, 8, 11 e 52, paragrafo 1, della Carta, dev'essere interpretato nel senso che il requisito secondo cui l'accesso da parte delle autorità nazionali competenti ai dati conservati dev'essere soggetto a un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente non è soddisfatto qualora una normativa nazionale preveda che un simile controllo sia effettuato dal pubblico ministero chiamato a dirigere il procedimento istruttorio e che possa al contempo rappresentare la pubblica accusa in giudizio.

V. Conclusione

130. Alla luce di quanto precede, propongo alla Corte di rispondere alle questioni sollevate dalla Riigikohus (Corte suprema, Estonia) nel modo seguente:

1) L'articolo 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, letto alla luce degli articoli 7, 8, 11 e 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, dev'essere interpretato nel senso che, tra i criteri che permettono di valutare la gravità dell'ingerenza nei diritti fondamentali costituita dall'accesso da parte delle autorità nazionali competenti a dati personali che i fornitori di servizi di comunicazione elettronica sono tenuti a conservare in forza di una normativa nazionale, rientrano le categorie di dati che vengono in rilievo nonché la durata del periodo con riferimento al quale tale accesso è richiesto. Compete al giudice del rinvio valutare, in funzione della gravità dell'ingerenza, se detto accesso fosse strettamente necessario in vista del raggiungimento dell'obiettivo di garantire la prevenzione, la ricerca, l'accertamento e il perseguimento dei reati.

2) L'articolo 15, paragrafo 1, della direttiva 2002/58, come modificata dalla direttiva 2009/136, letto alle luce degli articoli 7, 8, 11 e 52, paragrafo 1, della Carta dei diritti fondamentali, dev'essere interpretato nel senso che il requisito secondo cui l'accesso da parte delle autorità nazionali competenti ai dati conservati dev'essere soggetto a un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente non è soddisfatto qualora una normativa nazionale

preveda che un simile controllo sia effettuato dal pubblico ministero chiamato a dirigere il procedimento istruttorio e che possa al contempo rappresentare la pubblica accusa in giudizio.

1 Lingua originale: il francese.

2 GU 2002, L 201, pag. 37.

3 GU 2009, L 337, pag. 11. In prosieguo: la «direttiva 2002/58».

4 In prosieguo: la «Carta».

5 C-203/15 e C-698/15, EU:C:2016:970 [punto 120 e dispositivo, punto 2)]; in prosieguo: la «sentenza Tele2 Sverige e Watson e a.».

6 Direttiva del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU 1995, L 281, pag. 31).

7 RT I 2004, 87, 593.

8 RT I 2003, 27, 166.

9 RT I 1998, 41, 625.

10 Il giudice del rinvio precisa che, a seguito del cumulo di tale pena con la pena detentiva di quattro anni e sette mesi già irrogata con sentenza del 22 marzo 2016 del Viru Maakohus (Tribunale di primo grado di Viru), nei confronti di H.K. è stata inflitta, quale pena complessiva, una pena detentiva di cinque anni e un mese.

11 Si tratta del reato consistente nell'esercizio di un'influenza sulla giustizia. Rilevo che i fatti contestati a H.K., sotto tale profilo, sono stati riqualificati dal Viru Maakohus (Tribunale di primo grado di Viru), conformemente all'articolo 323, paragrafo 1, del codice penale, in violenza nei confronti delle parti di un procedimento giudiziario.

12 C-207/16, EU:C:2018:788; in prosieguo: la «sentenza Ministerio Fiscal».

13 Dispositivo, punto 2), di tale sentenza.

14 Punti 53 e 57 di tale sentenza.

15 Punti da 55 a 57 di tale sentenza.

16 Punto 120 e dispositivo, punto 2), di tale sentenza.

17 Il giudice del rinvio cita, al riguardo, le sentenze della Corte EDU del 2 settembre 2010, Uzun c. Germania (CE:ECHR:2010:0902JUD003562305, § da 71 a 74), e del 12 gennaio 2016, Szabó e Vissy c. Ungheria (CE:ECHR:2016:0112JUD003713814, § 77).

18 Sentenza Ministerio Fiscal (punto 34 e giurisprudenza ivi citata).

19 Idem.

20 Sentenza Ministerio Fiscal (punto 35 e giurisprudenza ivi citata).

21 Sentenza Ministerio Fiscal (punto 36 e giurisprudenza ivi citata).

22 Sentenza Ministerio Fiscal (punto 37 e giurisprudenza ivi citata).

23 V. sentenza Ministerio Fiscal (punti 38 e 39).

24 V. in particolare, per analogia, sentenza del 10 aprile 2003, Steffensen (C-276/01, EU:C:2003:228, punto 71). Nella citata sentenza, la Corte affronta tale problematica anche sotto il profilo del principio di effettività come limite all'autonomia procedurale degli Stati membri (punti da 66 a 68 di detta sentenza).

25 La Commissione sottolinea, in tale contesto, che la presente causa si distingue da quella che ha dato luogo alla sentenza Ministerio Fiscal.

26 V. sentenza Ministerio Fiscal (punti 49 e 50).

27 Sentenza Tele2 Sverige e Watson e a. (punto 112).

28 C-520/18, EU:C:2020:7. V., in particolare, paragrafi da 72 a 107 di tali conclusioni.

29 V. sentenza Tele2 Sverige e Watson e a. (punto 113).

30 V. sentenza Tele2 Sverige e Watson e a. (punto 115).

31 V. sentenza Tele2 Sverige e Watson e a. (punto 116).

32 Sentenza Tele2 Sverige e Watson e a. (punto 117).

33 Sentenza Tele2 Sverige e Watson e a. (punto 118).

34 Sentenza Tele2 Sverige e Watson e a. (punto 119).

35 Idem.

36 Sentenza Tele2 Sverige e Watson e a. (punto 120).

37 Idem.

38 Sentenza Tele2 Sverige e Watson e a. (punto 121).

39 V. sentenza Tele2 Sverige e Watson e a. (punto 122).

40 V. sentenza Ministerio Fiscal (punto 53).

41 Sentenza Ministerio Fiscal (punto 54).

42 Sentenza Ministerio Fiscal (punto 55).

43 Sentenza Ministerio Fiscal (punto 56).

44 Sentenza Ministerio Fiscal (punto 57).

45 Sentenza Ministerio Fiscal (punto 61).

46 Sentenza Ministerio Fiscal (punto 59).

47 Idem.

48 Sentenza Ministerio Fiscal (punto 60).

49 Sentenza Ministerio Fiscal (punto 62).

50 V. sentenza Ministerio Fiscal (punto 59). Nello stesso senso, v. conclusioni dell'avvocato generale Saugmandsgaard Øe nella causa Ministerio Fiscal (C-207/16, EU:C:2018:300), il quale osserva che la richiesta delle autorità di polizia riguardava «un periodo chiaramente definito e limitato nel tempo, vale a dire una dozzina di giorni» (paragrafo 33 nonché paragrafo 84).

51 Sentenza Ministerio Fiscal (punto 56).

52 Articolo 1111, paragrafo 11, della legge sulla comunicazione elettronica e articolo 901 del codice di procedura penale.

53 V. sentenza Ministerio Fiscal (punto 53).

54 Qualificato anche come «principio dell'ultima ratio».

55 Sentenza Tele2 Sverige e Watson e a. (punto 120 e giurisprudenza ivi citata); il corsivo è mio. Nello stesso senso, v. parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017 (EU:C:2017:592, punti 202 e 208).

56 V., in particolare, sentenza del 6 ottobre 2015, Schrems (C-362/14, EU:C:2015:650, punti 40 e 41 nonché giurisprudenza ivi citata). V., altresì, parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017 (EU:C:2017:592, punto 229).

57 Sentenza dell'8 aprile 2014, Commissione/Ungheria (C-288/12, EU:C:2014:237, punto 51 e giurisprudenza ivi citata).

58 Sentenza dell'8 aprile 2014, Commissione/Ungheria (C-288/12, EU:C:2014:237, punto 53 e giurisprudenza ivi citata).

59 V. sentenza del 9 ottobre 2019, NJ (Procura di Vienna) (C-489/19 PPU, EU:C:2019:849, punto 38 e giurisprudenza ivi citata).

60 V., da ultima, sentenza del 12 dicembre 2019, JR e YC (Procuratori di Lione e Tours e Procuratori di Lione e di Tours) (C-566/19 PPU e C-626/19 PPU, EU:C:2019:1077), nella quale la Corte ha considerato, in particolare, che gli elementi che le erano sottoposti erano sufficienti a dimostrare che, «in Francia, i magistrati della procura dispongono del potere di valutare in modo indipendente, segnatamente rispetto al potere esecutivo, la necessità e la proporzionalità dell'emissione di un mandato d'arresto europeo ed esercitano tale potere in modo oggettivo, tenendo conto di tutti gli elementi a carico e a discarico» (punto 55 di tale sentenza).

61 Sui due aspetti del requisito di indipendenza, v., per analogia, a proposito dei giudici nazionali chiamati a statuire su questioni legate all'interpretazione e all'applicazione del diritto dell'Unione, sentenza del 5 novembre 2019, Commissione/Polonia (Indipendenza dei tribunali ordinari) (C-192/18, EU:C:2019:924, punti da 108 a 110 nonché giurisprudenza ivi citata).

62 V., in particolare, sentenza del 27 maggio 2019, PF (Procuratore generale di Lituania) (C-509/18, EU:C:2019:457, punti 39 e 40).

63 Sentenza del 12 dicembre 1996, X (C-74/95 e C-129/95, EU:C:1996:491, punto 19).

64 Ad esempio, il pubblico ministero concede l'autorizzazione per l'osservazione in incognito di una persona, di una cosa o di un luogo, nonché, in molti casi, per la perquisizione.

65 V. altresì, nello stesso senso, articolo 30, paragrafo 2, del codice di procedura penale.

66 C-293/12 e C-594/12, EU:C:2014:238.

67 In base agli elementi presentati alla Corte in udienza, nel diritto estone tale controllo giurisdizionale può intervenire al termine della fase istruttoria, qualora una persona sospettata, che abbia preso visione del fascicolo, decida di contestare un atto relativo a tale fase, oppure in occasione del processo.