

SENTENZA DELLA CORTE (Grande Sezione)

2 ottobre 2018 (\*)

«Rinvio pregiudiziale – Comunicazioni elettroniche – Trattamento dei dati personali – Direttiva 2002/58/CE – Articoli 1 e 3 – Ambito di applicazione – Riservatezza delle comunicazioni elettroniche – Tutela – Articoli 5 e 15, paragrafo 1 – Carta dei diritti fondamentali dell’Unione europea – Articoli 7 e 8 – Dati raccolti nell’ambito della fornitura di servizi di comunicazione elettronica – Accesso delle autorità nazionali ai dati a fini di indagine – Soglia di gravità del reato che possa giustificare l’accesso ai dati»

Nella causa C-207/16,

avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell’articolo 267 TFUE, dall’Audiencia Provincial de Tarragona (Corte provinciale di Tarragona, Spagna), con decisione del 6 aprile 2016, pervenuta in cancelleria il 14 aprile 2016, nel procedimento avviato dal

**Ministerio Fiscal,**

LA CORTE (Grande Sezione),

composta da K. Lenaerts, presidente, A. Tizzano, vicepresidente, R. Silva de Lapuerta, T. von Danwitz (relatore), J.L. da Cruz Vilaça, C.G. Fernlund e C. Vajda, presidenti di sezione, E. Juhász, A. Borg Barthet, C. Toader, M. Safjan, D. Šváby, M. Berger, E. Jarašiūnas ed E. Regan, giudici,

avvocato generale: H. Saugmandsgaard Øe

cancelliere: L. Carrasco Marco, amministratore

vista la fase scritta del procedimento e in seguito all’udienza del 29 gennaio 2018,

considerate le osservazioni presentate:

- per il Ministerio Fiscal, da E. Tejada de la Fuente;
- per il governo spagnolo, da M. Sampol Pucurull, in qualità di agente;
- per il governo ceco, da M. Smolek, J. Vláčil e A. Brabcová, in qualità di agenti;
- per il governo danese, da J. Nymann-Lindgren e M. Wolff, in qualità di agenti;
- per il governo estone, da N. Grünberg, in qualità di agente;
- per l’Irlanda, da M. Browne, L. Williams, E. Creedon e A. Joyce, in qualità di agenti, assistiti da E. Gibson, BL;
- per il governo francese, da D. Colas, E. de Moustier ed E. Armoet, in qualità di agenti;
- per il governo lettone, da I. Kucina e J. Davidoviča, in qualità di agenti;
- per il governo ungherese, da M. Fehér e G. Koós, in qualità di agenti;
- per il governo austriaco, da C. Pesendorfer, in qualità d’agente;
- per il governo polacco, da B. Majczyna, D. Lutostańska e J. Sawicka, in qualità di agenti;
- per il governo del Regno Unito, da S. Brandon e C. Brodie, in qualità di agenti, assistiti da C. Knight, barrister, e G. Facenna, QC;
- per la Commissione europea, da I. Martínez del Peral, P. Costa de Oliveira, R. Troosters e D. Nardi, in qualità di agenti,

sentite le conclusioni dell'avvocato generale, presentate all'udienza del 3 maggio 2018,

ha pronunciato la seguente

### **Sentenza**

1 La domanda di pronuncia pregiudiziale verte, in sostanza, 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) (GU 2002, L 201, pag. 37), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009 (GU 2009, L 337, pag. 11) (in prosieguo: la «direttiva 2002/58»), letta alla luce degli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»).

2 Tale domanda è stata proposta nell'ambito di un ricorso presentato dal Ministerio Fiscal (pubblico ministero, Spagna) avverso la decisione dello Juzgado de Instrucción n. 3 de Tarragona (giudice istruttore n. 3 di Tarragona; in prosieguo: il «giudice istruttore»), recante rifiuto di autorizzare l'accesso della polizia giudiziaria a dati personali conservati da fornitori di servizi di comunicazione elettronica.

### **Contesto normativo**

#### ***Diritto dell'Unione***

##### *Direttiva 95/46*

3 Ai sensi dell'articolo 2, lettera b), della direttiva 95/46/CE 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), ai fini di quest'ultima, per «trattamento di dati personali» si deve intendere «qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione».

4 L'articolo 3 di tale direttiva, intitolato «Ambito di applicazione» prevede quanto segue:

«1. Le disposizioni della presente direttiva si applicano al trattamento di dati personali interamente o parzialmente automatizzato nonché al trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi.

2. Le disposizioni della presente direttiva non si applicano ai trattamenti di dati personali:

- effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del trattato sull'Unione europea e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale;
- effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico».

##### *Direttiva 2002/58*

5 I considerando 2, 11, 15 e 21 della direttiva 2002/58 così recitano:

«(2) La presente direttiva mira a rispettare i diritti fondamentali e si attiene ai principi riconosciuti in particolare dalla [Carta]. In particolare, la presente direttiva mira a garantire il pieno rispetto dei diritti di cui agli articoli 7 e 8 di [quest'ultima].

(...)

(11) La presente direttiva, analogamente alla direttiva [95/46], non affronta le questioni relative alla tutela dei diritti e delle libertà fondamentali inerenti ad attività che non sono disciplinate dal diritto comunitario. Lascia pertanto inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti di cui all'articolo 15, paragrafo 1, della presente direttiva, necessari per tutelare 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) e l'applicazione della legge penale. Di conseguenza la presente direttiva non pregiudica la facoltà degli Stati membri di effettuare intercettazioni legali di comunicazioni elettroniche o di prendere altre misure, se necessario, per ciascuno di tali scopi e conformemente alla Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali, come interpretata dalle sentenze della Corte europea dei diritti dell'uomo. Tali misure devono essere appropriate, strettamente proporzionate allo scopo perseguito, necessarie in una società democratica ed essere soggette ad idonee garanzie conformemente alla precitata Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

(...)

(15) Una comunicazione può comprendere qualsiasi informazione relativa al nome, al numero e all'indirizzo fornita da chi emette la comunicazione o dall'utente di un collegamento al fine di effettuare la comunicazione. I dati relativi al traffico possono comprendere qualsiasi traslazione dell'informazione da parte della rete sulla quale la comunicazione è trasmessa allo scopo di effettuare la trasmissione. (...)

(...)

(21) Occorre prendere misure per prevenire l'accesso non autorizzato alle comunicazioni al fine di tutelare la riservatezza delle comunicazioni realizzate attraverso reti pubbliche di comunicazione e servizi di comunicazione elettronica accessibili al pubblico compreso il loro contenuto e qualsiasi dato ad esse relativo. La legislazione di alcuni Stati membri vieta soltanto l'accesso intenzionale non autorizzato alle comunicazioni».

6 L'articolo 1 della direttiva 2002/58, intitolato «Finalità e campo d'applicazione», così dispone:

«1. La presente direttiva prevede l'armonizzazione delle disposizioni nazionali necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata e alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno della Comunità.

2. Ai fini di cui al paragrafo 1, le disposizioni della presente direttiva precisano e integrano la direttiva [95/46]. Esse prevedono inoltre la tutela dei legittimi interessi degli abbonati che sono persone giuridiche.

3. La presente direttiva 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 L'articolo 2 della direttiva 2002/58, intitolato «Definizioni», è del seguente tenore:

«Salvo diversa disposizione, ai fini della presente direttiva si applicano le definizioni di cui alla direttiva [95/46] e alla direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica (direttiva quadro) [(GU 2002, L 108, pag. 33)].

Si applicano inoltre le seguenti definizioni:

(...)

b) “dati relativi al traffico”: qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

c) “dati relativi all’ubicazione”: ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indichi la posizione geografica dell’apparecchiatura terminale dell’utente di un servizio di comunicazione elettronica accessibile al pubblico;

d) “comunicazione”: ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse, come parte di un servizio di radiodiffusione, al pubblico tramite una rete di comunicazione elettronica salvo quando le informazioni possono essere collegate all’abbonato o utente che riceve le informazioni che può essere identificato;

(...».

8 L’articolo 3 della direttiva 2002/58, intitolato «Servizi interessati», prevede quanto segue:

«La presente direttiva si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche nella Comunità, comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati».

9 L’articolo 5 della direttiva 2002/58, intitolato «Riservatezza delle comunicazioni», è del seguente tenore:

«1. Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite [una] rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare essi vietano l’ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell’articolo 15, paragrafo 1. (...)

(...)

3. Gli Stati membri assicurano che l’archiviazione di informazioni oppure l’accesso a informazioni già archiviate nell’apparecchiatura terminale di un abbonato o di un utente sia consentito unicamente a condizione che l’abbonato o l’utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, a norma della direttiva [95/46], tra l’altro sugli scopi del trattamento. (...».

10 L’articolo 6 della direttiva 2002/58, intitolato «Dati sul traffico», dispone quanto segue:

«1. I dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, fatti salvi i paragrafi 2, 3 e 5 del presente articolo e l’articolo 15, paragrafo 1.

2. I dati relativi al traffico che risultano necessari ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione possono essere sottoposti a trattamento. Tale trattamento è consentito solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento.

(...».

11 L'articolo 15, paragrafo 1, della citata direttiva, intitolato «Applicazione di alcune disposizioni della direttiva [95/46]», enuncia quanto segue:

«Gli 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], 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 comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea».

### ***Diritto spagnolo***

#### *La legge n. 25/2007*

12 L'articolo 1 della Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a la redes públicas de comunicaciones (legge n. 25/2007, sulla conservazione dei dati relativi alle comunicazioni elettroniche e alle reti pubbliche di comunicazione), del 18 ottobre 2007 (BOE n. 251, del 19 ottobre 2007, pag. 42517), dispone quanto segue:

«1. La presente legge disciplina l'obbligo degli operatori di conservare i dati generati o trattati nell'ambito della prestazione di servizi di comunicazione elettronica o di reti pubbliche di comunicazione nonché il dovere di cedere tali dati agli agenti, muniti, ogni volta che ciò sia loro richiesto, di una corrispondente autorizzazione dell'autorità giudiziaria, a fini di accertamento, indagine e perseguimento di reati gravi previsti dal codice penale o da leggi penali speciali.

2. La presente legge si applica ai dati relativi al traffico e ai dati relativi all'ubicazione delle persone sia fisiche che giuridiche, nonché ai dati connessi necessari per identificare l'abbonato o l'utente registrato.

(...».

#### *Il codice penale*

13 L'articolo 13, paragrafo 1, della Ley Orgánica 10/1995 del Código Penal (codice penale), del 23 novembre 1995 (BOE n. 281, del 24 novembre 1995, pag. 33987), è formulato come segue:

«Sono considerati reati gravi quelli che la legge punisce con una pena grave».

14 L'articolo 33 di detto codice prevede quanto segue:

«1. In funzione della loro natura e della loro durata, le pene si distinguono in gravi, meno gravi e lievi.

2. Sono pene gravi:

a) l'ergastolo.

b) la reclusione superiore a cinque anni.

(...)».

#### *Il codice di procedura penale*

15 Successivamente alla data dei fatti di cui al procedimento principale, la Ley de Enjuiciamiento Criminal (codice di procedura penale) è stato modificato dalla Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (legge organica 13/2015 che modifica il codice di procedura penale allo scopo di rafforzare le garanzie processuali e disciplinare i mezzi di investigazione tecnologici), del 5 ottobre 2015 (BOE n. 239, del 6 ottobre 2015, pag. 90192).

16 Questa legge è entrata in vigore il 6 dicembre 2015. Essa inserisce nel codice di procedura penale le disposizioni riguardanti l'accesso ai dati relativi alle comunicazioni telefoniche e telematiche conservati dai fornitori di servizi di comunicazione elettronica.

17 L'articolo 579, paragrafo 1, del codice di procedura penale, nella versione derivante dalla legge organica 13/2015, prevede quanto segue:

«1. Il giudice può autorizzare l'intercettazione della corrispondenza privata, postale e telegrafica, compresi i telefax, i Buofax e i vaglia postali internazionali, che l'indagato invii o riceva, nonché l'apertura e l'analisi di quest'ultima qualora sussistano indizi che inducano a ritenere che essa consenta di scoprire o accertare un fatto o un fattore rilevante per la causa, purché l'indagine abbia ad oggetto uno dei seguenti reati:

- 1) reati dolosi puniti con una pena detentiva massima non inferiore a tre anni.
- 2) reati commessi nell'ambito di un'organizzazione criminale.
- 3) reati di terrorismo.

(...)».

18 L'articolo 588 ter j di detto codice prevede quanto segue:

«1. I dati elettronici conservati dai prestatori di servizi o da persone che agevolano la comunicazione in applicazione della normativa sulla conservazione dei dati relativi alle comunicazioni elettroniche o di propria iniziativa per motivi commerciali o di altra natura, e che siano collegati a processi di comunicazione, possono essere ceduti per essere acquisiti al processo soltanto su autorizzazione del giudice.

2. Qualora la conoscenza di tali dati sia indispensabile per le indagini, viene chiesta al giudice competente un'autorizzazione per raccogliere le informazioni contenute negli archivi automatizzati dei prestatori di servizi, compresa la ricerca incrociata o intelligente di dati, a condizione che vengano precisate la natura dei dati da raccogliere e le ragioni che giustificano la cessione».

#### **Procedimento principale e questioni pregiudiziali**

19 Il sig. Hernández Sierra ha presentato una denuncia alla polizia per una rapina, avvenuta il 16 febbraio 2015, nel corso della quale è stato ferito e gli sono stati rubati il portafoglio e il telefono cellulare.

20 Il 27 febbraio 2015, la polizia giudiziaria ha chiesto al giudice istruttore di ordinare a vari fornitori di servizi di comunicazione elettronica la trasmissione dei numeri di telefono attivati, tra il 16 febbraio e il 27 febbraio 2015, con il codice relativo all'identificatore internazionale apparecchiature mobili (in prosieguo: il «codice IMEI») del telefono cellulare rubato e i dati personali relativi all'identità civile dei titolari o utenti

dei numeri di telefono corrispondenti alle carte SIM attivate con detto codice, quali il loro cognome, nome e, se del caso, indirizzo.

21 Con ordinanza del 5 maggio 2015 il giudice istruttore ha respinto tale domanda. Da una parte, egli ha stabilito che la misura richiesta non era utile per identificare gli autori del reato. Dall'altra parte, egli ha rifiutato di accogliere la domanda con la motivazione che la legge 25/2007 limitava la comunicazione dei dati conservati dai fornitori di servizi di comunicazione elettronica ai reati gravi. Ai sensi del codice penale i reati gravi sono punibili con pene detentive superiori a cinque anni, mentre i fatti di cui trattasi nel procedimento principale non sembra che integrino gli estremi di un tale reato.

22 Il pubblico ministero ha interposto appello avverso tale ordinanza dinanzi al giudice del rinvio, sostenendo che la comunicazione dei dati in questione avrebbe dovuto essere concessa in ragione della natura dei fatti e di una decisione del Tribunal Supremo (Corte suprema, Spagna), del 26 luglio 2010, riguardante un caso simile.

23 Il giudice del rinvio spiega che, dopo l'adozione di tale ordinanza, il legislatore spagnolo ha modificato il codice di procedura penale con l'adozione della legge organica 13/2015. Tale legge, che sarebbe rilevante per l'esito del ricorso principale, avrebbe introdotto due criteri alternativi nuovi per determinare il livello di gravità di un reato. Si tratterebbe, da una parte, di un criterio materiale individuato da comportamenti tipici che corrispondono a qualificazioni penali di specifica e grave rilevanza criminosa e che sono anche particolarmente lesivi dei beni giuridici individuali e collettivi. Dall'altra parte, il legislatore nazionale avrebbe fatto ricorso a un criterio normativo formale, fondato sulla pena prevista per il reato in questione. La soglia di tre anni di reclusione adesso prevista da questo criterio comprenderebbe, tuttavia, la maggior parte dei reati. Inoltre, il giudice del rinvio ritiene che l'interesse dello Stato a reprimere i comportamenti penalmente illeciti non possa giustificare ingerenze sproporzionate nei diritti fondamentali previsti dalla Carta.

24 A tal riguardo, detto giudice considera che, nel procedimento principale, le direttive 95/46 e 2002/58 stabilirebbero il collegamento con la Carta. La normativa nazionale di cui trattasi nel procedimento principale rientrerebbe pertanto, ai sensi dell'articolo 51, paragrafo 1, della Carta, nell'ambito di applicazione di essa, nonostante l'annullamento della direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (GU 2006, L 105, pag. 54), da parte della sentenza dell'8 aprile 2014, Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238).

25 In tale sentenza, la Corte avrebbe affermato che la conservazione e la comunicazione dei dati relativi al traffico costituiscono ingerenze particolarmente gravi nei diritti garantiti dagli articoli 7 e 8 della Carta, e avrebbe identificato i criteri di valutazione del rispetto del principio di proporzionalità, tra cui la gravità dei reati che giustifica la conservazione di tali dati e l'accesso a essi a fini investigativi.

26 È alla luce di tali circostanze che l'Audiencia Provincial de Tarragona (Corte provinciale di Tarragona) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se la soglia di sufficiente gravità dei reati, quale criterio che giustifica l'ingerenza nei diritti fondamentali riconosciuti dagli articoli 7 e 8 della Carta, possa essere individuata prendendo in considerazione unicamente la pena irrogabile per il reato oggetto di indagini o se sia inoltre necessario rilevare nella condotta criminosa particolari livelli di lesività nei confronti dei beni giuridici individuali e/o collettivi.

2) Qualora la determinazione della gravità del reato sulla sola base della pena irrogabile risultasse conforme ai principi costituzionali dell'Unione, applicati dalla Corte nell'ambito della sentenza [dell'8 aprile

2014, Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238], quali parametri di controllo rigoroso della direttiva [2002/58], quale dovrebbe essere tale soglia, e se essa risulti compatibile con una previsione generale di un limite di tre anni di reclusione».

### **Procedimento dinanzi alla Corte**

27 Con decisione del presidente della Corte del 23 maggio 2016, il procedimento dinanzi a essa è stato sospeso fino alla pronuncia della sentenza nelle cause riunite Tele2 Sverige e Watson e a., C-203/15 e C-698/15 (sentenza del 21 dicembre 2016, EU:C:2016:970; in prosieguo: la «sentenza Tele2 Sverige e Watson e a.»). In seguito alla pronuncia di tale sentenza, al giudice del rinvio è stato chiesto se intendesse confermare o ritirare la sua domanda di pronuncia pregiudiziale. In risposta, esso ha, con lettera del 30 gennaio 2017, pervenuta in cancelleria il 14 febbraio 2017, comunicato che tale sentenza non gli permetteva di valutare, con sufficiente certezza, la normativa nazionale di cui trattasi nel procedimento principale ai sensi del diritto dell'Unione. Pertanto, il procedimento dinanzi alla Corte veniva ripreso il 16 febbraio 2017.

### **Sulle questioni pregiudiziali**

28 Il governo spagnolo eccepisce, da una parte, l'incompetenza della Corte a rispondere alla domanda di pronuncia pregiudiziale e, dall'altra parte, l'irricevibilità di tale domanda.

### **Sulla competenza della Corte**

29 Nelle sue osservazioni scritte sottoposte alla Corte, il governo spagnolo ha espresso il parere, condiviso dal governo del Regno Unito durante l'udienza, secondo il quale la Corte non sarebbe competente a rispondere alla domanda di pronuncia pregiudiziale poiché il procedimento principale è, ai sensi dell'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46 e dell'articolo 1, paragrafo 3, della direttiva 2002/58, escluso dall'ambito di applicazione di queste due direttive. Tale causa non rientrerebbe dunque nell'ambito di applicazione del diritto dell'Unione, e quindi la Carta, ai sensi del suo articolo 51, paragrafo 1, non sarebbe applicabile.

30 Secondo il governo spagnolo, la Corte ha certo statuito, nella sentenza Tele2 Sverige e Watson e a., che una misura legislativa che disciplina l'accesso delle autorità nazionali ai dati conservati dai fornitori di servizi di comunicazione elettronica rientra nell'ambito di applicazione della direttiva 2002/58. Nel caso di specie, tuttavia, si tratterebbe di una domanda di accesso di un'autorità pubblica, in forza di una decisione giudiziaria nell'ambito di un procedimento istruttorio penale, a dati personali conservati dai fornitori di servizi di comunicazione elettronica. Il governo spagnolo ne trae la conclusione che tale domanda di accesso rientri nell'esercizio, da parte delle autorità nazionali, dello ius puniendi, con la conseguenza che essa costituisce un'attività dello Stato in materia di diritto penale che rientra nell'eccezione prevista all'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46 e all'articolo 1, paragrafo 3, della direttiva 2002/58.

31 Al fine di valutare l'eccezione di incompetenza, bisogna rilevare che l'articolo 1 della direttiva 2002/58 dispone, al suo paragrafo 1, che essa prevede l'armonizzazione delle disposizioni nazionali necessarie per assicurare, segnatamente, un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata e alla riservatezza, riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche. Ai sensi del suo articolo 1, paragrafo 2, tale direttiva precisa e completa la direttiva 95/46 ai fini enunciati a detto paragrafo 1.

32 L'articolo 1, paragrafo 3, della direttiva 2002/58 esclude dal proprio ambito di applicazione le «attività dello Stato» nei settori ivi indicati, tra i quali figurano le attività dello Stato in settori del diritto penale e quelle 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 (sentenza Tele2 Sverige e

Watson e a., punto 69 e giurisprudenza ivi citata). Le attività in esso menzionate a titolo esemplificativo sono, in tutti i casi, attività proprie degli Stati o delle autorità statali, estranee ai settori di attività dei privati (v., per analogia, per quanto riguarda l'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46, sentenza del 10 luglio 2018, *Jehovan Todistajat*, C-25/17, EU:C:2018:551, punto 38 e giurisprudenza ivi citata).

33 L'articolo 3 della direttiva 2002/58 enuncia che detta direttiva si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche nell'Unione, comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati (in prosieguo: i «servizi di comunicazione elettronica»). Pertanto, la citata direttiva deve essere considerata come disciplinante le attività dei fornitori di tali servizi (sentenza *Tele2 Sverige e Watson e a.*, punto 70).

34 Per quanto concerne l'articolo 15, paragrafo 1, della direttiva 2002/58, la Corte ha già statuito che le misure legislative previste da questa disposizione 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. 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 (v., in tal senso, sentenza *Tele2 Sverige e Watson e a.*, punti da 72 a 74).

35 La Corte ha concluso 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 (v., in tal senso, sentenza *Tele2 Sverige e Watson e a.*, punti 75 e 76).

36 Infatti, 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 (sentenza *Tele2 Sverige e Watson e a.*, punto 77).

37 Va 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 (v., in tal senso, sentenza *Tele2 Sverige e Watson e a.*, punti da 75 a 78). 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.

38 Nel caso di specie, come risulta dalla decisione di rinvio, la domanda di cui al procedimento principale, con cui la polizia giudiziaria chiede un'autorizzazione giudiziaria per l'accesso a dati personali conservati da alcuni fornitori di servizi di comunicazioni elettroniche, ha come fondamento la legge 25/2007, letta in combinato disposto con il codice di procedura penale, nella versione applicabile ai fatti di cui al procedimento principale, che disciplina l'accesso delle autorità pubbliche a tali dati. Tale normativa

permette alla polizia giudiziaria, in caso di concessione dell'autorizzazione giudiziaria richiesta sul fondamento della suddetta legge, di imporre ai fornitori di servizi di comunicazione elettronica di rendere disponibili dati personali e permette, in tal modo, che essi procedano, alla luce della definizione di cui all'articolo 2, lettera b), della direttiva 95/46, applicabile nell'ambito della direttiva 2002/58 ai sensi dell'articolo 2, primo comma, di quest'ultima, a un «trattamento» di tali dati in virtù delle suddette due direttive. La citata normativa, pertanto, disciplina le attività dei fornitori di servizi di comunicazione elettronica e rientra, di conseguenza, nell'ambito di applicazione della direttiva 2002/58.

39 Alla luce di quanto precede, la circostanza dedotta dal governo spagnolo, secondo cui tale domanda di accesso interviene nel contesto della fase istruttoria di un procedimento penale, non può rendere la direttiva 2002/58 inapplicabile alla fattispecie di cui al procedimento principale, in virtù dell'articolo 1, paragrafo 3, della stessa.

40 A tal riguardo è altresì irrilevante che la domanda di accesso di cui trattasi nel procedimento principale, come emerge dalla risposta scritta del governo spagnolo a un quesito posto dalla Corte, e come confermato da tale governo e dal pubblico ministero in udienza, miri a permettere l'accesso ai soli numeri di telefono corrispondenti alle carte SIM attivate con il codice IMEI del telefono cellulare rubato e ai dati relativi all'identità civile dei titolari di tali carte, quali il loro cognome, nome e, se del caso, indirizzo, ad esclusione dei dati relativi alle comunicazioni effettuate con tali schede SIM e dei dati relativi all'ubicazione del telefono cellulare rubato.

41 Infatti, come rilevato dall'avvocato generale al paragrafo 54 delle sue conclusioni, la direttiva 2002/58 disciplina, in forza del suo articolo 1, paragrafo 1, e del suo articolo 3, qualsiasi trattamento di dati personali nell'ambito della fornitura di servizi di comunicazione elettronica. Inoltre, ai sensi dell'articolo 2, secondo comma, lettera b), di tale direttiva, la nozione di «dati relativi al traffico» comprende «qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione».

42 A tal proposito, per quanto riguarda, più in particolare, i dati riguardanti l'identità civile dei titolari di carte SIM, risulta dal considerando 15 della direttiva 2002/58 che i dati relativi al traffico possono comprendere, in particolare, il nome e l'indirizzo della persona che emette una comunicazione o che utilizza un collegamento al fine di effettuare una comunicazione. I dati relativi all'identità civile dei titolari delle carte SIM possono, inoltre, rivelarsi necessari per la fatturazione dei servizi di comunicazione elettronica forniti e fanno pertanto parte dei dati relativi al traffico, come definiti nell'articolo 2, secondo comma, lettera b), di tale direttiva. Questi dati rientrano quindi nell'ambito di applicazione della direttiva 2002/58.

43 La Corte è pertanto competente a risolvere la questione sollevata dal giudice del rinvio.

#### ***Sulla ricevibilità***

44 Il governo spagnolo sostiene che la domanda di pronuncia pregiudiziale è irricevibile poiché non identifica chiaramente le disposizioni del diritto dell'Unione sulle quali la Corte è chiamata a pronunciarsi. Inoltre, la domanda della polizia giudiziaria di cui trattasi nel procedimento principale non concernerebbe l'intercettazione delle comunicazioni effettuate tramite carte SIM attivate con il codice IMEI del telefono cellulare rubato, ma riguarderebbe un collegamento tra tali carte e i loro titolari, con la conseguenza che non si inciderebbe sulla riservatezza delle comunicazioni. L'articolo 7 della Carta menzionato nelle questioni pregiudiziali non sarebbe quindi pertinente nell'ambito della presente causa.

45 Secondo costante giurisprudenza della Corte, spetta esclusivamente al giudice nazionale, cui è stata sottoposta la controversia e che deve assumersi la responsabilità della futura decisione giurisdizionale, valutare, alla luce delle particolari circostanze di ciascuna causa, sia la necessità di una pronuncia

pregiudiziale per essere in grado di pronunciare la propria sentenza, sia la rilevanza delle questioni che esso sottopone alla Corte. Di conseguenza, purché le questioni sollevate riguardino l'interpretazione del diritto dell'Unione, la Corte, in via di principio, è tenuta a statuire. Il rifiuto della Corte di statuire su una questione pregiudiziale sollevata da un giudice nazionale è possibile solo quando appaia in modo manifesto che l'interpretazione del diritto dell'Unione chiesta non ha alcuna relazione con la realtà materiale o con l'oggetto della causa principale, qualora il problema sia di natura teorica oppure, ancora, qualora la Corte non disponga degli elementi di fatto o di diritto necessari per fornire una soluzione utile alle questioni che le vengono sottoposte (sentenza del 10 luglio 2018, Jehovan Todistajat, C-25/17, EU:C:2018:551, punto 31 e giurisprudenza ivi citata).

46 Nel caso di specie, la decisione di rinvio contiene elementi di fatto e di diritto sufficienti sia per l'identificazione delle disposizioni del diritto dell'Unione richiamate nelle questioni pregiudiziali sia per comprendere la portata di dette questioni. In particolare, risulta dalla decisione di rinvio che le questioni pregiudiziali sono destinate a consentire al giudice del rinvio di valutare se, e in quale misura, la normativa nazionale, sulla quale è fondata la domanda della polizia giudiziaria di cui trattasi nel procedimento principale, persegue un obiettivo che possa giustificare una limitazione dei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta. Orbene, secondo le indicazioni dello stesso giudice, detta normativa nazionale rientra nell'ambito di applicazione della direttiva 2002/58, cosicché la Carta è applicabile al procedimento principale. Le questioni pregiudiziali presentano pertanto un rapporto diretto con l'oggetto della controversia principale e, di conseguenza, non possono essere considerate di natura teorica.

47 Alla luce di quanto precede le questioni pregiudiziali sono ricevibili.

#### ***Nel merito***

48 Con le sue due questioni, che è opportuno esaminare congiuntamente, il giudice del rinvio chiede, in sostanza, se l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7 e 8 della Carta, debba essere interpretato nel senso che l'accesso delle autorità pubbliche ai dati che mirano all'identificazione dei titolari di carte SIM attivate con un telefono cellulare rubato, come il cognome, il nome e, se del caso, l'indirizzo di tali titolari, comporta un'ingerenza nei diritti fondamentali di questi ultimi, sanciti dai suddetti articoli della Carta, che presenta una gravità tale da dover limitare il suddetto accesso, in materia di prevenzione, ricerca, accertamento e perseguimento dei reati, alla lotta contro la criminalità grave e, in caso affermativo, sulla base di quali criteri dovrebbe essere valutata la gravità dell'infrazione in questione.

49 A tal riguardo, emerge dalla decisione di rinvio che, come rilevato in sostanza dall'avvocato generale al paragrafo 38 delle sue conclusioni, la domanda di pronuncia pregiudiziale non mira 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 e 8 della Carta. Tale domanda verte, come emerge dal punto 46 della presente sentenza, esclusivamente sulla questione se e in quale misura l'obiettivo perseguito dalla normativa di cui trattasi nel procedimento principale sia idoneo a giustificare l'accesso delle pubbliche autorità, come la polizia giudiziaria, a tali dati, senza che le altre condizioni di accesso risultanti da tale articolo 15, paragrafo 1, siano oggetto della suddetta domanda.

50 In particolare, tale giudice si interroga sugli elementi da prendere in considerazione al fine di determinare se i reati con riferimento ai quali le autorità di polizia possono essere autorizzate, a fini di indagine, ad accedere a dati personali conservati dai fornitori di servizi di comunicazioni elettroniche, siano tanto gravi da giustificare l'ingerenza che un tale accesso comporta nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta, come interpretati dalla Corte nelle sue sentenze dell'8 aprile 2014, Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238), e Tele2 Sverige e Watson e a.

51 Per quanto riguarda l'esistenza di un'ingerenza in tali diritti fondamentali, occorre ricordare che, come rilevato dall'avvocato generale ai paragrafi 76 e 77 delle sue conclusioni, l'accesso delle autorità pubbliche a tali dati costituisce un'ingerenza nel diritto fondamentale al rispetto della vita privata, sancito all'articolo 7 della Carta, persino in mancanza di circostanze che permettano di qualificare tale ingerenza come «grave» e senza che rilevi il fatto che le informazioni in questione relative alla vita privata siano o meno delicate o che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a tale ingerenza. Tale accesso costituisce anche un'ingerenza nel diritto fondamentale alla protezione dei dati personali garantito dall'articolo 8 della Carta, poiché costituisce un trattamento di dati personali [v., in tal senso, parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punti 124 e 126 e giurisprudenza ivi citata].

52 Per quanto riguarda gli obiettivi idonei a giustificare una normativa nazionale, come quella di cui trattasi nel procedimento principale, che disciplina l'accesso delle autorità pubbliche ai dati conservati dai fornitori di servizi di comunicazioni elettroniche e che derogano pertanto al principio della riservatezza delle comunicazioni elettroniche, occorre ricordare che l'elenco degli obiettivi di cui all'articolo 15, paragrafo 1, primo periodo, della direttiva 2002/58 ha carattere tassativo, di modo che tale accesso deve rispondere in modo effettivo e rigoroso ad uno di questi obiettivi (v., in tal senso, sentenza Tele2 Sverige e Watson e a., punti 90 e 115).

53 Orbene, per quanto riguarda l'obiettivo di prevenzione, ricerca, accertamento e perseguimento dei reati, occorre rilevare che la formulazione dell'articolo 15, paragrafo 1, primo periodo, della direttiva 2002/58 non limita tale obiettivo alla lotta contro i soli reati gravi, ma si riferisce ai «reati» in generale.

54 A tal proposito, la Corte 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 (v., in tal senso, sentenza Tele2 Sverige e Watson e a., punto 99).

55 Tuttavia, la Corte ha motivato tale interpretazione affermando che l'obiettivo perseguito da una normativa che disciplina tale accesso deve essere adeguata alla gravità dell'ingerenza nei diritti fondamentali in questione che tale operazione determina (v., in tal senso, sentenza Tele2 Sverige e Watson e a., punto 115).

56 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».

57 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.

58 È pertanto opportuno, innanzitutto, determinare se, nel caso di specie, in base alle circostanze del caso, l'ingerenza nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta, che un accesso della polizia giudiziaria ai dati di cui trattasi nel procedimento principale comporterebbe, debba essere considerata come «grave».

59 A tal riguardo, la domanda di cui al procedimento principale attraverso la quale la polizia giudiziaria chiede, ai fini di un'indagine penale, l'autorizzazione giudiziaria per l'accesso a dati personali conservati da alcuni fornitori di servizi di comunicazioni elettroniche, ha il solo scopo di identificare i titolari delle carte SIM attivate, per un periodo di dodici giorni, con il codice IMEI del telefono cellulare rubato. Come rilevato al precedente punto 40, tale domanda riguarda l'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 riguardano, come confermato sia dal governo spagnolo sia dal pubblico ministero in udienza, le comunicazioni effettuate con il telefono cellulare rubato o l'ubicazione di quest'ultimo.

60 Risulta quindi 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.

61 In tali circostanze, l'accesso ai soli dati oggetto della domanda di cui trattasi nel procedimento principale non può essere qualificato come un'ingerenza «grave» nei diritti fondamentali delle persone i cui dati sono oggetto di attenzione.

62 Come risulta dai punti da 53 a 57 della presente sentenza, l'ingerenza che un accesso a tali dati comporterebbe può quindi essere giustificata dall'obiettivo di prevenzione, ricerca, accertamento e perseguimento di «reati» in generale, di cui all'articolo 15, paragrafo 1, primo periodo, della direttiva 2002/58, senza che sia necessario che tali reati siano qualificati come «gravi».

63 Alla luce delle suesposte considerazioni, occorre rispondere alle questioni poste dichiarando che l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7 e 8 della Carta, deve essere interpretato nel senso che l'accesso delle autorità pubbliche ai dati che mirano all'identificazione dei titolari di carte SIM attivate con un telefono cellulare rubato, come il cognome, il nome e, se del caso, l'indirizzo di tali titolari, comporta un'ingerenza nei diritti fondamentali di questi ultimi, sanciti dai suddetti articoli della Carta, che non presenta una gravità tale da dover limitare il suddetto accesso, in materia di prevenzione, ricerca, accertamento e perseguimento dei reati, alla lotta contro la criminalità grave.

#### **Sulle spese**

64 Nei confronti delle parti nel procedimento principale la presente causa costituisce un incidente sollevato dinanzi al giudice nazionale, cui spetta quindi statuire sulle spese. Le spese sostenute da altri soggetti per presentare osservazioni alla Corte non possono dar luogo a rifusione.

Per questi motivi, la Corte (Grande Sezione) dichiara:

**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 e 8 della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che l'accesso delle autorità pubbliche ai dati che mirano all'identificazione dei titolari di carte SIM attivate con un telefono cellulare rubato, come il cognome, il nome e, se del caso, l'indirizzo di tali titolari, comporta un'ingerenza nei diritti fondamentali di questi ultimi, sanciti dai suddetti articoli della Carta dei diritti fondamentali, che non presenta una gravità tale da dover limitare il suddetto accesso, in materia di prevenzione, ricerca, accertamento e perseguimento dei reati, alla lotta contro la criminalità grave.**

Firme