



## Raccolta della giurisprudenza

CONCLUSIONI DELL'AVVOCATO GENERALE  
MANUEL CAMPOS SÁNCHEZ-BORDONA  
presentate il 18 novembre 2021<sup>1</sup>

**Cause riunite C-793/19 e C-794/19**

**Bundesrepublik Deutschland**  
**contro**

**SpaceNet AG (C-793/19)**  
**Telekom Deutschland GmbH (C-794/19)**

[domanda di pronuncia pregiudiziale proposta dal Bundesverwaltungsgericht (Corte amministrativa federale, Germania)]

«Domanda di pronuncia pregiudiziale – Telecomunicazioni – Trattamento dei dati personali e protezione della vita privata nel settore delle comunicazioni elettroniche – Direttiva 2002/58/CE – Articolo 15, paragrafo 1 – Articolo 4, paragrafo 2, TUE – Carta dei diritti fondamentali dell'Unione europea – Articoli 6, 7, 8, 11 e 52, paragrafo 1 – Conservazione generalizzata e indifferenziata dei dati di connessione ai fini della repressione dei reati gravi o della prevenzione di un rischio concreto per la sicurezza nazionale»

1. Le presenti domande di pronuncia pregiudiziale, alle quali si aggiunge quella della causa C-140/20<sup>2</sup>, evidenziano, ancora una volta, la preoccupazione suscitata in alcuni Stati membri dalla giurisprudenza della Corte in materia di conservazione e accesso ai dati personali generati nel settore delle comunicazioni elettroniche.

2. Nelle conclusioni relative alle cause C-511/18 e C-512/18, *La Quadrature du Net e a.*<sup>3</sup>, e C-520/18, *Ordre des barreaux francophones et germanophone e a.*<sup>4</sup>, ho indicato quali tappe più importanti di tale giurisprudenza, fino ad allora, quelle seguenti:

– la sentenza dell'8 aprile 2014, *Digital Rights Ireland e a.*<sup>5</sup>, che ha dichiarato l'invalidità della direttiva 2006/24/CE<sup>6</sup> in quanto comportava un'ingerenza non proporzionata nei diritti sanciti dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»);

<sup>1</sup> Lingua originale: lo spagnolo.

<sup>2</sup> C-140/20, *Commissioner of the Garda Síochána e a.*, sulla quale presento parimenti le mie conclusioni in data odierna.

<sup>3</sup> In prosieguo: le «conclusioni *La Quadrature du Net*» (EU:C:2020:6).

<sup>4</sup> In prosieguo: le «conclusioni *Ordre des barreaux francophones et germanophone*» (EU:C:2020:7).

<sup>5</sup> C-293/12 e C-594/12 (EU:C:2014:238; in prosieguo: la «sentenza *Digital Rights*»).

<sup>6</sup> Direttiva 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).

- la sentenza del 21 dicembre 2016, *Tele2 Sverige e Watson e a.*<sup>7</sup>, in cui è stato dichiarato che l'articolo 15, paragrafo 1, della direttiva 2002/58/CE<sup>8</sup> osta ad una normativa nazionale che preveda una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione per finalità di lotta contro le forme gravi di criminalità;
- la sentenza del 2 ottobre 2018, *Ministerio Fiscal*<sup>9</sup>, che ha confermato l'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58, precisando l'importanza a tale riguardo del principio di proporzionalità.

3. Nel 2018 taluni giudici di alcuni Stati membri si sono rivolti alla Corte, nelle rispettive domande di pronuncia pregiudiziale, esprimendo i loro dubbi sulla questione se tali sentenze (del 2014, 2016 e 2018) potessero privare le autorità statali di uno strumento necessario per la salvaguardia della sicurezza nazionale e la lotta contro la criminalità e il terrorismo.

4. Quattro di dette domande di pronuncia pregiudiziale hanno dato luogo alle sentenze *Privacy International*<sup>10</sup> e *La Quadrature du Net e a.*<sup>11</sup>, entrambe del 6 ottobre 2020, che hanno sostanzialmente confermato la giurisprudenza della sentenza *Tele2 Sverige*, pur introducendo alcune sfumature aggiuntive.

5. Per la loro provenienza (la Grande Sezione della Corte), il loro contenuto e il loro intento di illustrare nel dettaglio, in dialogo con i giudici del rinvio, i motivi che, nonostante tutto, giustificano le tesi ivi esposte, ci si potrebbe attendere che queste due sentenze «riepilogative» del 6 ottobre 2020 abbiano risolto il dibattito. A qualsiasi altra domanda di pronuncia pregiudiziale sul medesimo argomento corrisponderebbe quindi un'ordinanza motivata ai sensi dell'articolo 99 del regolamento di procedura della Corte di giustizia.

6. Tuttavia, prima del 6 ottobre 2020 erano pervenute presso la cancelleria della Corte altre tre domande di pronuncia pregiudiziale (le due riunite nel presente procedimento e quella della causa C-140/20), il cui contenuto metteva nuovamente in discussione la giurisprudenza elaborata in merito all'articolo 15, paragrafo 1, della direttiva 2002/58.

7. La Corte ha comunicato ai giudici del rinvio le sentenze del 6 ottobre 2020, affinché essi ritirassero, se lo volevano, le domande di pronuncia pregiudiziale. Dinanzi alla loro volontà di mantenerle, come spiegherò nel prosieguo<sup>12</sup>, è stato deciso di non applicare l'articolo 99 del regolamento di procedura e di lasciare che la Grande Sezione della Corte risponda a tali questioni.

<sup>7</sup> C-203/15 e C-698/15 (EU:C:2016:970; in prosieguo: la «sentenza *Tele2 Sverige*»).

<sup>8</sup> Direttiva 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).

<sup>9</sup> C-207/16 (EU:C:2018:788).

<sup>10</sup> C-623/17 (EU:C:2020:790).

<sup>11</sup> C-511/18, C-512/18 e C-520/18 (EU:C:2020:791; in prosieguo: la «sentenza *La Quadrature du Net*»).

<sup>12</sup> Paragrafo 30 delle presenti conclusioni.

## I. Contesto normativo

### A. Diritto dell'Unione. Direttiva 2002/58

8. Ai sensi dell'articolo 5 («Riservatezza delle comunicazioni»), paragrafo 1:

«Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la 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. Questo paragrafo non impedisce la memorizzazione tecnica necessaria alla trasmissione della comunicazione fatto salvo il principio della riservatezza».

9. L'articolo 6 («Dati sul traffico») così dispone:

«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.

(...)».

10. L'articolo 15 («Applicazione di alcune disposizioni della direttiva 95/46/CE»)<sup>13</sup>, prevede, al paragrafo 1, 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/CE, 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».

<sup>13</sup> 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).

## **B. Diritto nazionale**

### *1. Telekommunikationsgesetz (legge relativa alle telecomunicazioni; in prosieguo: il «TKG»)*

11. L'articolo 113a, paragrafo 1, così recita:

«Gli obblighi concernenti la conservazione, l'utilizzo e la sicurezza dei dati relativi al traffico definiti negli articoli da 113b a 113g riguardano gli operatori che forniscono agli utenti finali servizi di telecomunicazione accessibili al pubblico».

12. L'articolo 113b prevede quanto segue:

«(1) Gli operatori di cui all'articolo 113a devono conservare i dati nel territorio nazionale nel modo seguente:

1. per dieci settimane nel caso dei dati di cui ai paragrafi 2 e 3,
  2. per quattro settimane nel caso dei dati relativi all'ubicazione di cui al paragrafo 4.
- (2) I fornitori di servizi di telefonia accessibili al pubblico conservano
1. il numero di telefono o altro identificativo della linea chiamante e della linea chiamata, nonché di ogni altra linea utilizzata in caso di commutazione o trasferimento di chiamata,
  2. la data e l'ora di inizio e fine del collegamento con indicazione del relativo fuso orario,
  3. le indicazioni del servizio utilizzato, qualora possano essere utilizzati diversi servizi nell'ambito della telefonia,
  4. nel caso della telefonia mobile, inoltre
    - a) l'identificativo internazionale degli abbonati alla telefonia mobile per la linea chiamante e la linea chiamata,
    - b) l'identificativo internazionale dell'apparecchiatura terminale chiamante e chiamata,
    - c) la data e l'ora della prima attivazione del servizio con indicazione del relativo fuso orario, in caso di servizi prepagati,
  5. nel caso di telefonia via Internet, anche gli indirizzi IP (protocollo Internet) della linea chiamante e della linea chiamata e gli identificativi di utente attribuiti.

Il primo comma si applica mutatis mutandis

1. in caso di comunicazione tramite SMS, messaggio multimediale o simile; in tal caso, le indicazioni di cui al primo comma, punto 2, sono sostituite dall'ora di invio e di ricezione del messaggio;
2. alle chiamate senza risposta o non riuscite per un intervento dell'operatore di rete (...).

(3) I fornitori di servizi di accesso a Internet accessibili al pubblico conservano

1. l'indirizzo IP assegnato all'abbonato ai fini dell'uso di Internet,
2. l'identificativo univoco della linea attraverso la quale ha luogo l'uso di Internet, nonché l'identificativo di utente attribuito,
3. la data e l'ora di inizio e fine dell'uso di Internet dall'indirizzo IP assegnato, con indicazione del relativo fuso orario.

(4) In caso di utilizzo di servizi di telefonia mobile deve essere conservata l'indicazione delle celle telefoniche utilizzate all'inizio del collegamento da chi effettua la chiamata e da chi la riceve. Per quanto riguarda i servizi di accesso a Internet accessibili al pubblico, deve essere conservata, in caso di uso mobile, l'indicazione delle celle telefoniche utilizzate all'inizio della connessione a Internet. Devono inoltre essere conservati i dati che permettono di conoscere la posizione geografica e le direzioni di radiazione massima delle antenne che servono la cella telefonica in questione.

(5) Non possono essere conservati ai sensi della presente disposizione il contenuto della comunicazione, i dati relativi ai siti Internet consultati e i dati dei servizi di posta elettronica.

(6) Non possono essere conservati ai sensi della presente disposizione i dati alla base delle comunicazioni di cui all'articolo 99, paragrafo 2. Ciò vale, mutatis mutandis, per le comunicazioni telefoniche provenienti dagli enti di cui all'articolo 99, paragrafo 2. Si applica mutatis mutandis l'articolo 99, paragrafo 2, frasi dalla seconda alla settima <sup>[14]</sup>.

(...)).

13. A tenore dell'articolo 113c:

«(1) I dati conservati a norma dell'articolo 113b possono

1. essere trasmessi a un'autorità repressiva quando ne richieda la trasmissione in forza di una disposizione di legge che la autorizzi a raccogliere i dati di cui all'articolo 113b ai fini della repressione di reati di particolare gravità;
2. essere trasmessi a un'autorità di sicurezza dei Länder quando ne richieda la trasmissione in forza di una disposizione di legge che la autorizzi a raccogliere i dati di cui all'articolo 113b ai fini della prevenzione di un rischio concreto per l'integrità fisica, la vita o la libertà di una persona o per l'esistenza dello Stato federale o del Land;
3. essere utilizzati dal fornitore di servizi di telecomunicazione accessibili al pubblico per la comunicazione di informazioni ai sensi dell'articolo 113, paragrafo 1, terza frase.

<sup>14</sup> Le comunicazioni di cui all'articolo 99, paragrafo 2 del TKG sono comunicazioni con persone, autorità e organizzazioni di carattere sociale o religioso che offrono agli interlocutori, in linea di principio anonimi, servizi di assistenza telefonica in casi di situazioni di urgenza psicologica o sociale e che sono soggette a particolari obblighi di riservatezza. Ai sensi dell'articolo 99, paragrafo 2, frasi dalla seconda alla quarta, del TKG, tale eccezione è subordinata all'iscrizione in un elenco gestito dalla Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Agenzia federale per le reti di elettricità, gas, telecomunicazioni, posta e ferrovie, Germania; in prosieguo: l'«Agenzia federale delle reti»), previo accreditamento della natura dei loro servizi mediante certificazione rilasciata da un ente, da un organismo o da una fondazione di diritto pubblico.

(2) I dati conservati a norma dell'articolo 113b non possono essere utilizzati da persone soggette agli obblighi stabiliti all'articolo 113a, paragrafo 1, per finalità diverse da quelle previste al paragrafo 1.

(...)).

14. Ai sensi dell'articolo 113d:

«Il destinatario dell'obbligo di cui all'articolo 113a, paragrafo 1, deve garantire che i dati conservati conformemente all'articolo 113b, paragrafo 1, in base all'obbligo di conservazione siano protetti, con misure tecniche e organizzative conformi allo stato della tecnica, da controlli e usi non autorizzati. Tali misure comprendono in particolare:

1. l'utilizzo di una procedura di crittografia particolarmente sicura,
2. la conservazione in infrastrutture di conservazione distinte, separate da quelle destinate alle normali funzioni operative,
3. la conservazione, con un livello elevato di protezione contro gli attacchi informatici, in sistemi informatici scollegati di trattamento dei dati,
4. la limitazione dell'accesso agli impianti utilizzati per il trattamento dei dati alle persone in possesso di un'autorizzazione speciale rilasciata dal titolare dell'obbligo e
5. l'obbligo di far intervenire, durante l'accesso ai dati, almeno due persone in possesso di un'autorizzazione speciale rilasciata dal responsabile dell'obbligo».

15. L'articolo 113e così recita:

«(1) Il responsabile dell'obbligo di cui all'articolo 113a, paragrafo 1, deve garantire che, ai fini del controllo della protezione dei dati, sia registrato, in virtù dell'obbligo di conservazione, ogni accesso, e in particolare la lettura, la copiatura, la modifica, la cancellazione e la chiusura, ai dati conservati conformemente all'articolo 113b, paragrafo 1. Devono essere registrati

1. l'ora dell'accesso,
2. le persone che accedono ai dati,
3. lo scopo e la natura dell'accesso.

(2) I dati registrati non possono essere utilizzati per finalità diverse dal controllo della protezione dei dati.

(3) Il responsabile dell'obbligo di cui all'articolo 113a, paragrafo 1, deve garantire che i dati registrati siano cancellati dopo un anno».

## 2. *Strafprozessordnung* (codice di procedura penale; in prosieguo: la «StPO»)

16. L'articolo 100g stabilisce quanto segue:

«(...)

(2) Qualora determinate circostanze inducano a sospettare che una persona abbia commesso, come autore o complice, uno dei reati particolarmente gravi di cui alla seconda frase o, nei casi in cui sia punibile il tentativo di reato, abbia tentato di commetterlo e se il reato è particolarmente grave anche nel singolo caso, i dati relativi al traffico, conservati conformemente all'articolo 113b del [TKG], possono essere raccolti se l'indagine sui fatti o la localizzazione della persona indagata sarebbero eccessivamente difficili o impossibili con altri mezzi e la raccolta dei dati è proporzionata all'importanza della questione.

(...)

(4) Non è consentita la raccolta dei dati relativi al traffico ai sensi del paragrafo 2 (...) che possa portare a informazioni sulle quali l'interessato potrebbe rifiutarsi di testimoniare (...)».

17. L'articolo 101a, paragrafo 1, sottopone a un'autorizzazione giudiziaria la raccolta di dati relativi al traffico ai sensi dell'articolo 100g della StPO. A norma dell'articolo 101a, paragrafo 2, del medesimo codice, la decisione giudiziaria deve valutare la necessità e la pertinenza nel singolo caso della misura, la cui adozione deve essere resa nota ai partecipanti alla comunicazione (articolo 101, paragrafo 6, della StPO).

## II. Fatti, controversie e questioni pregiudiziali

18. La SpaceNet AG e la Telekom Deutschland GmbH sono società che forniscono, nella Repubblica federale di Germania, servizi di accesso a Internet accessibili al pubblico.

19. Le due società suddette hanno adito il Verwaltungsgericht (Tribunale amministrativo, Germania) opponendosi all'obbligo di conservare i dati relativi al traffico delle telecomunicazioni dei loro clienti a decorrere dal 1° luglio 2017, imposto dall'articolo 113a, paragrafo 1, in combinato disposto con l'articolo 113b, del TKG.

20. In seguito all'accoglimento delle loro rispettive domande in primo grado, l'Agenzia federale delle reti ha presentato due ricorsi per cassazione («Revision») dinanzi al Bundesverwaltungsgericht (Corte amministrativa federale), il quale, prima di pronunciarsi, ha deciso di sollevare in entrambi i procedimenti la seguente questione pregiudiziale:

«Se l'articolo 15 della direttiva 2002/58/CE, alla luce degli articoli 7, 8 e 11, nonché 52, paragrafo 1, della Carta (...), da un lato, e dell'articolo 6 della Carta medesima, nonché dell'articolo 4 [TUE], dall'altro, debba essere interpretato nel senso che osti ad una normativa nazionale, la quale obblighi i fornitori di servizi di comunicazione elettronica accessibili al pubblico a conservare i dati relativi al traffico e all'ubicazione degli utenti finali di detti servizi, laddove

– tale obbligo non presupponga alcun motivo specifico di ordine locale, temporale o spaziale,

- costituiscano oggetto dell'obbligo di memorizzazione, nella fornitura di servizi telefonici accessibili al pubblico – inclusa la trasmissione di messaggi di testo (SMS), multimediali (MMS) o simili, nonché le chiamate senza risposta oppure non riuscite – i seguenti dati:
  - il numero di telefono o altro identificativo della linea chiamante e della linea chiamata, nonché di ogni altra linea interessata in caso di commutazione o trasferimento di chiamata,
  - la data e l'ora di inizio e fine del collegamento o – nel caso di trasmissione di un messaggio di testo (SMS), multimediale (MMS) o simile – le date della spedizione e della ricezione del messaggio con indicazione del relativo fuso orario,
  - indicazione del servizio utilizzato, qualora possano essere utilizzati diversi servizi nell'ambito della telefonia,
  - nel caso di telefonia mobile, inoltre
    - l'identificativo internazionale degli abbonati alla telefonia mobile per la linea chiamante e la linea chiamata,
    - l'identificativo internazionale dell'apparecchiatura terminale chiamante e chiamata,
    - data e ora della prima attivazione del servizio con indicazione del relativo fuso orario, in caso di servizi prepagati,
    - l'indicazione delle celle telefoniche utilizzate dalla linea chiamante e dalla linea chiamata all'inizio del collegamento,
  - nel caso di telefonia via Internet, anche gli indirizzi di protocollo Internet della linea chiamante e della linea chiamata e gli identificativi di utente attribuiti,
- costituiscano oggetto dell'obbligo di memorizzazione, nella fornitura di servizi di accesso a Internet accessibili al pubblico, i seguenti dati:
  - l'indirizzo di protocollo Internet assegnato all'abbonato ai fini dell'uso di Internet,
  - l'identificativo univoco della linea attraverso la quale ha luogo l'uso di Internet, nonché l'identificativo di utente attribuito,
  - data e ora di inizio e fine dell'uso di Internet con l'indirizzo di protocollo Internet assegnato con indicazione del relativo fuso orario,
  - in caso di uso mobile, l'indicazione della cella telefonica utilizzata all'inizio del collegamento a Internet,
- i seguenti dati non possano essere memorizzati:
  - il contenuto della comunicazione,
  - dati relativi alla pagina Internet visitata,
  - dati dei servizi di posta elettronica,

- dati relativi ai collegamenti in uscita o in entrata da determinate linee di persone, autorità e organizzazioni in ambito sociale o religioso,
- la durata della conservazione di dati relativi all'ubicazione, vale a dire l'indicazione della cella telefonica utilizzata, sia pari a quattro settimane e, per gli altri dati, a dieci settimane,
- sia assicurata un'efficace protezione dei dati conservati contro i rischi di abuso e di accesso non autorizzato, e
- i dati conservati possano essere utilizzati solo ai fini del perseguimento di reati particolarmente gravi o della prevenzione di un pericolo concreto per la vita, l'integrità fisica o la libertà di una persona ovvero ai fini della salvaguardia dello Stato o di un Land (Regione), ad eccezione degli indirizzi di protocollo Internet assegnati all'abbonato per l'uso di Internet, il cui utilizzo sia consentito nell'ambito di un accesso ai dati archiviati finalizzato al perseguimento di eventuali reati, al mantenimento dell'ordine e della sicurezza pubblici, nonché all'assolvimento dei compiti dei servizi di intelligence».

21. Secondo le spiegazioni fornite dal giudice del rinvio, la disciplina dell'obbligo controverso è stata modificata da una legge del 10 dicembre 2015<sup>15</sup>, la cui adozione era necessaria dopo:

- la sentenza del Bundesverfassungsgericht (Corte costituzionale federale, Germania) del 2 marzo 2010<sup>16</sup>, che ha dichiarato incostituzionali le disposizioni anteriori relative alla conservazione dei dati, e
- la declaratoria di nullità della direttiva 2006/24, per il cui recepimento erano state adottate tali disposizioni.

22. Il giudice del rinvio ritiene che l'obbligo di conservazione controverso comporti una restrizione dei diritti di cui all'articolo 5, paragrafo 1, all'articolo 6, paragrafo 1, e all'articolo 9, paragrafo 1, della direttiva 2002/58. A suo avviso, detta restrizione sarebbe giustificata solo qualora potesse essere consentita ai sensi dell'articolo 15, paragrafo 1, di tale direttiva.

23. Secondo il giudice del rinvio, nonostante la giurisprudenza della sentenza Tele2 Sverige, l'obbligo oggetto della controversia potrebbe trovare fondamento nell'articolo 15, paragrafo 1, della direttiva 2002/58, in quanto:

- le norme nazionali applicabili non richiedono la memorizzazione di tutti i dati sul traffico relativo alle telecomunicazioni di *tutti* gli utenti e abbonati con riguardo a *tutti* i mezzi di comunicazione elettronica;
- tali norme hanno drasticamente ridotto (fino a un massimo di dieci settimane) la durata della memorizzazione, rispetto a quella prevista dalle normative esaminate nella sentenza Tele2 Sverige e a quella contemplata dalla direttiva 2006/24, il che rende più difficile la profilazione;
- sono state imposte severe restrizioni per quanto riguarda la protezione e l'utilizzo dei dati memorizzati e l'accesso ad essi;

<sup>15</sup> Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (legge istitutiva dell'obbligo e di un periodo massimo di memorizzazione di dati sul traffico).

<sup>16</sup> 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 (DE:BVVerfG:2010:rs20100302.1bvr025608).

- il legislatore si sarebbe limitato ad adempiere gli obblighi di intervento imposti dal diritto alla sicurezza (articolo 6 della Carta)<sup>17</sup>;
- qualora una conservazione «ingiustificata»<sup>18</sup> dei dati non potesse essere fondata, in via generale, sull'articolo 15, paragrafo 1, della direttiva 2002/58 (vale a dire, qualora siano irrilevanti le norme specifiche riguardanti i mezzi di comunicazione interessati, le categorie di dati da memorizzare, la durata della memorizzazione, le condizioni di accesso ai dati memorizzati e la protezione contro i rischi di abuso), ne risulterebbe notevolmente limitato il margine di manovra dei legislatori nazionali in un ambito che, come quello del perseguimento dei reati e della sicurezza pubblica, continua ad essere, ai sensi dell'articolo 4, paragrafo 2, terza frase, TUE, di esclusiva competenza di ciascuno Stato membro;
- deve essere assicurata la coerenza tra i diritti garantiti dalla Carta e quelli sanciti dalla Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (in prosieguo: la «CEDU»), interpretati dalla Corte europea dei diritti dell'uomo (in prosieguo: la «Corte EDU»), fatte salve l'autonomia del diritto dell'Unione e l'autorità della Corte di giustizia.

### III. Procedimento dinanzi alla Corte

24. Le domande di pronuncia pregiudiziale sono pervenute alla cancelleria della Corte il 29 ottobre 2019.

25. Hanno presentato osservazioni scritte la SpaceNet, la Telekom Deutschland, i governi danese, dei Paesi Bassi, estone, finlandese, francese, irlandese, polacco, spagnolo, svedese e tedesco, nonché la Commissione.

26. Invitato a pronunciarsi sull'eventuale ritiro delle questioni pregiudiziali dopo la pronuncia della sentenza *La Quadrature du Net*, il 13 gennaio 2021, il giudice del rinvio ha manifestato l'intenzione di mantenerle, in quanto non potevano essere considerate risolte da tale sentenza.

27. All'udienza pubblica, comune alla causa connessa C-140/20, tenutasi il 13 settembre 2021 sono intervenuti, oltre alle parti che hanno presentato osservazioni scritte nel presente procedimento, l'Agenzia federale delle reti e il Garante europeo della protezione dei dati.

### IV. Analisi

#### A. Considerazioni preliminari

28. Le due domande di pronuncia pregiudiziale in esame possono essere trattate sia analizzandole come sono state presentate inizialmente sia tenendo conto prevalentemente delle considerazioni adottate dal giudice del rinvio nella risposta alla Corte del 13 gennaio 2021 per giustificarne il mantenimento, dopo aver avuto cognizione della sentenza *La Quadrature du Net*.

<sup>17</sup> Secondo il giudice del rinvio, la giurisprudenza della Corte non preclude categoricamente ai legislatori nazionali la possibilità, sulla base di una valutazione complessiva, di introdurre la conservazione ingiustificata dei dati (eventualmente integrata da rigorose norme di accesso), al fine di tener conto dello specifico potenziale di rischio associato ai nuovi mezzi di telecomunicazione.

<sup>18</sup> Tale è l'espressione letterale utilizzata dal giudice del rinvio.

29. Anche se affronterò brevemente i punti più rilevanti delle domande di pronuncia pregiudiziale originarie, mi concentrerò sull'analisi dei motivi per i quali, ad avviso del giudice del rinvio, continua ad essere necessario l'intervento della Corte. In sintesi, tutti i suddetti motivi si fondano sul fatto che la situazione normativa di base è diversa da quella esaminata nella sentenza *La Quadrature du Net*.

30. Nella sua comunicazione del 13 gennaio 2021, il giudice del rinvio ha addotto le seguenti argomentazioni:

- le differenze tra le norme tedesche e quelle francesi e belghe oggetto della sentenza *La Quadrature du Net* sono significative. Secondo le prime, non vengono conservati i dati relativi ai siti Internet consultati, quelli della posta elettronica e quelli inerenti alle comunicazioni da o verso servizi di assistenza telefonica di carattere sociale o religioso.
- Un'altra differenza ancor più significativa consiste nel fatto che la durata della conservazione, ai sensi dell'articolo 113b, paragrafo 1, del TKG è di quattro o dieci settimane, e non di un anno. Tale fattore riduce il rischio che si possa tracciare un profilo complessivo degli interessati.
- Le norme tedesche offrono una protezione efficace dei dati conservati contro i pericoli di abuso e di accesso illecito.
- In seguito a una recente pronuncia del Bundesverfassungsgericht (Corte costituzionale federale) sull'articolo 113 del TKG<sup>19</sup>, la validità di tale disposizione sarebbe subordinata a condizioni di cui non sarebbe facile determinare la compatibilità con il diritto dell'Unione.
- Permangono incertezze sui requisiti del diritto dell'Unione relativi agli indirizzi IP, in quanto la sentenza *La Quadrature du Net* non consente di stabilire chiaramente se la loro conservazione sia esclusa in generale, dal momento che si ravvisa una certa conflittualità tra i punti 168 e 155 di tale sentenza.

### ***B. Applicabilità della direttiva 2002/58***

31. La Repubblica d'Irlanda e i governi dei Paesi Bassi, francese, polacco e svedese sostengono, in sostanza, che la direttiva 2002/58 non si applica a normative nazionali come quella di cui trattasi nei presenti procedimenti. Poiché hanno ad oggetto la salvaguardia della sicurezza nazionale nonché la prevenzione e la repressione dei reati gravi, dette normative rientrano nella competenza esclusiva degli Stati membri, conformemente all'articolo 4, paragrafo 2, TUE.

32. Tale obiezione è stata respinta, in modo chiaro, dalla Corte nella sentenza *La Quadrature du Net* dichiarando che «una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica di conservare dati relativi al traffico e dati relativi all'ubicazione a fini di salvaguardia della sicurezza nazionale e di lotta alla criminalità, quali le normative di cui trattasi nei procedimenti principali, rientra nell'ambito di applicazione della direttiva 2002/58»<sup>20</sup>.

<sup>19</sup> Sentenza del 27 maggio 2020, 1 BvR 1873/13, 1 BvR 2618/13 (DE:BVerfG:2020:rs20200527.1bvr187313). Secondo detta sentenza, l'articolo 113 del TKG è incompatibile con gli articoli 2, paragrafo 1, e 10, paragrafo 1, del Grundgesetz (Legge fondamentale) e può essere applicato solo fino all'adozione di nuove norme, al più tardi sino al 31 dicembre 2021.

<sup>20</sup> Sentenza *La Quadrature du Net*, punto 104.

33. Il giudice del rinvio accoglie tale premessa confermando la valutazione del giudice di primo grado e aggiungendo che l'applicabilità della direttiva 2005/58 nel caso di specie era stata «stabilita definitivamente» dalla sentenza Tele2 Sverige<sup>21</sup>.

34. Non mi soffermerò quindi su questo punto, riguardo al quale ho avuto occasione di esprimermi a suo tempo, sulla stessa linea assunta dalla Corte, nelle conclusioni La Quadrature du Net<sup>22</sup>.

### ***C. Conservazione generalizzata e indifferenziata contro conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione***

35. L'idea chiave della giurisprudenza della Corte relativa alla direttiva 2002/58 è che gli utenti dei mezzi di comunicazione elettronica hanno il diritto di attendersi, in linea di principio, che le loro comunicazioni e i dati a queste correlati rimangano anonimi e non possano essere registrati, salvo loro consenso<sup>23</sup>.

36. L'articolo 15, paragrafo 1, della direttiva 2002/58 ammette deroghe all'obbligo di garantire la riservatezza e agli obblighi corrispondenti, nei termini che riporterò più avanti. La sentenza La Quadrature du Net si sofferma sulla conciliazione di tali deroghe con i diritti fondamentali il cui esercizio potrebbe essere leso<sup>24</sup>.

37. La conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione potrebbe essere giustificata, secondo la Corte, solo dall'obiettivo della salvaguardia della sicurezza nazionale, la cui importanza «supera quella degli altri obiettivi di cui all'articolo 15, paragrafo 1, della direttiva 2002/58»<sup>25</sup>.

38. In tal caso (sicurezza nazionale), la Corte ha dichiarato che l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta, «non osta, in linea di principio, a una misura legislativa che autorizzi le autorità competenti ad imporre ai fornitori di servizi di comunicazione elettronica di procedere alla *conservazione* dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli utenti dei mezzi di comunicazione elettronica *per un periodo limitato*, se ricorrono circostanze sufficientemente concrete che consentono di ritenere che lo Stato membro interessato affronti una minaccia grave (...) per la sicurezza nazionale che si rivela reale e attuale o prevedibile»<sup>26</sup>.

39. Tali prescrizioni determinano certamente un regime più rigoroso e restrittivo di quello risultante dalla giurisprudenza della Corte EDU relativa all'articolo 8 della CEDU. Il fatto che il «significato e la portata» dei diritti della Carta corrispondenti a quelli della CEDU debbano essere uguali a quelli conferiti da quest'ultima non preclude, ai sensi dell'articolo 52, paragrafo 3, in fine, della Carta, che il diritto dell'Unione conceda una protezione più estesa.

<sup>21</sup> Punto 19, lettera a), della decisione di rinvio.

<sup>22</sup> Conclusioni La Quadrature du Net, paragrafi da 40 a 90.

<sup>23</sup> Sentenza La Quadrature du Net, punto 109.

<sup>24</sup> Ibidem, punti da 111 a 133.

<sup>25</sup> Sentenza La Quadrature du Net, punto 136.

<sup>26</sup> Ibidem, punto 137 (il corsivo è mio). Ciò vale, prosegue la Corte, «[a]nche se una misura siffatta riguarda, in maniera indifferenziata, tutti gli utenti di mezzi di comunicazione elettronica senza che questi ultimi sembrino, a prima vista, presentare alcun collegamento (...) con una minaccia per la sicurezza nazionale di tale Stato membro», dovendosi quindi «considerare che l'esistenza di una simile minaccia è idonea, di per sé, a stabilire detto collegamento» (ibidem).

40. Inoltre, la giurisprudenza elaborata dalla Corte EDU nelle sentenze del 25 maggio 2021, *Big Brother Watch e a. c. Regno Unito*<sup>27</sup> e *Centrum för Rättvisa c. Svezia*<sup>28</sup>, nonché in quella del 4 dicembre 2015, *Zakharov c. Russia*<sup>29</sup>, riguarda casi che, come è stata la posizione prevalente tra le parti in udienza, non sono equiparabili a quelli in discussione nei presenti rinvii pregiudiziali. In questi ultimi, la soluzione va cercata applicando normative nazionali ritenute conformi alla disciplina *esaustiva* della direttiva 2002/58, come interpretata dalla Corte.

41. A prescindere dal parere sul richiamo alla sicurezza nazionale, nella sentenza *La Quadrature du Net*, in quanto motivo per derogare, a determinate condizioni, al divieto di conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione (a mio avviso, i limiti posti dalla Corte sono eccessivamente ampi), devono essere rispettate le prescrizioni elencate ai punti da 137 a 139 di detta sentenza.

42. Al di fuori di tale ipotesi, occorrerà esaminare se la disciplina nazionale si basi su criteri sufficientemente *mirati* per rispettare le condizioni che, secondo la giurisprudenza della Corte, possono giustificare un'ingerenza particolarmente grave, quale la conservazione di dati, nei diritti fondamentali interessati.

43. La *conservazione mirata* dei dati relativi al traffico e dei dati relativi all'ubicazione<sup>30</sup> è la pietra angolare del ragionamento delle sentenze della Corte in materia. Tale selezione può essere effettuata in funzione delle categorie di persone interessate<sup>31</sup> o basarsi su un criterio geografico<sup>32</sup>, tra altri.

44. Sia il giudice del rinvio che la maggioranza delle parti che hanno presentato osservazioni hanno evidenziato le difficoltà implicate dai criteri indicati dalla Corte. Io stesso ho segnalato alcune di tali difficoltà<sup>33</sup> nelle conclusioni *Ordre des barreaux francophones et germanophone*<sup>34</sup>.

45. Tuttavia, non si può escludere che formule di conservazione mirata basate su tali criteri risultino efficaci e, allo stesso tempo, non discriminatorie. Spetta ai legislatori nazionali, e non alla Corte di giustizia, elaborarle in modo da rispettare i diritti fondamentali garantiti dalla Carta<sup>35</sup>.

46. Ribadisco, inoltre, che sarebbe errato dedurre che i criteri personale e geografico siano gli unici compatibili con l'articolo 15, paragrafo 1, della direttiva 2002/58, alla luce dei diritti tutelati dalla Carta.

<sup>27</sup> CE:ECHR:2021:0525JUD005817013.

<sup>28</sup> CE:ECHR:2021:0525JUD003525208.

<sup>29</sup> CE:ECHR:2015:1204JUD004714306.

<sup>30</sup> Sentenza *La Quadrature du Net*, punto 147: «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, non osta a che uno Stato membro adotti una normativa la quale consenta, a titolo preventivo, una *conservazione mirata* dei dati relativi al traffico e dei dati relativi all'ubicazione, per finalità di lotta contro la criminalità grave e di prevenzione delle minacce gravi alla sicurezza pubblica, nonché a fini di salvaguardia della sicurezza nazionale, a condizione che tale conservazione sia, per quanto concerne le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone riguardate, nonché la durata di conservazione prevista, limitata allo stretto necessario». Il corsivo è mio.

<sup>31</sup> Sentenza *La Quadrature du Net*, punti 148 e 149.

<sup>32</sup> Sentenza *La Quadrature du Net*, punto 150.

<sup>33</sup> Oltre alla loro insufficienza, la possibilità che essi conducano all'instaurazione di un regime di sospetto generale su taluni segmenti della popolazione o alla stigmatizzazione di zone geografiche.

<sup>34</sup> Conclusioni *Ordre des barreaux francophones et germanophone*, paragrafi 88 e 89.

<sup>35</sup> *Ibidem*, paragrafo 90.

47. Sebbene il governo francese sostenga che si sono dimostrate inefficaci<sup>36</sup>, ritengo che non si possano neanche escludere le modalità proposte dai gruppi di lavoro riuniti in seno al Consiglio<sup>37</sup> per definire norme di conservazione e di accesso compatibili con la giurisprudenza della Corte<sup>38</sup>.

48. A mio avviso, si dovrebbe preferire una conservazione temporanea di alcune *categorie* di dati relativi al traffico e all'ubicazione, limitate in funzione delle strette esigenze di sicurezza, che non consentano, nel loro insieme, di ottenere un'immagine precisa e dettagliata della vita degli interessati. A livello pratico, ciò significa che, tra le due categorie principali (dati relativi al traffico e dati relativi all'ubicazione), devono essere conservati, mediante gli opportuni filtri, soltanto i dati *minimi* ritenuti assolutamente indispensabili per la prevenzione e il controllo efficaci della criminalità e per la salvaguardia della sicurezza nazionale<sup>39</sup>.

49. Ad ogni modo, ripeto, spetta agli Stati membri o alle istituzioni dell'Unione effettuare, per via legislativa (con l'assistenza dei rispettivi esperti), siffatta selezione, rinunciando a qualsiasi tentativo di imporre una conservazione generalizzata e indifferenziata di tutti i dati relativi al traffico e all'ubicazione<sup>40</sup>.

50. Per tale motivo ho affermato nelle conclusioni *Ordre des barreaux francophones et germanophone* che «[l]a difficoltà legislativa – che riconosco – di definire con precisione i casi e le condizioni in cui si possa effettuare una conservazione mirata non giustifica il fatto che gli Stati membri, facendo dell'eccezione una norma, trasformino la conservazione generalizzata di dati personali nel principio chiave della loro legislazione. Se così fosse, si ammetterebbe la durata a tempo indeterminato di un pregiudizio rilevante al diritto alla protezione dei dati personali»<sup>41</sup>.

#### ***D. Punto 168 della sentenza La Quadrature du Net***

51. In tale contesto, gli elementi indispensabili per rispondere al giudice del rinvio derivano, a mio avviso, direttamente dalla giurisprudenza della Corte relativa all'articolo 15, paragrafo 1, della direttiva 2002/58, come riepilogata nella sentenza *La Quadrature du Net*.

52. Devo quindi rammentare, anzitutto, la giurisprudenza elaborata dalla Corte nella suddetta sentenza, il cui punto 168 la riassume come segue:

«[L]’articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 e dell’articolo 52, paragrafo 1, della Carta, deve essere interpretato nel senso che osta a misure legislative che prevedono, ai fini di cui all’articolo 15, paragrafo 1, a titolo preventivo, una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all’ubicazione. Per contro, l’articolo 15, paragrafo 1, letto alla luce degli articoli 7, 8 e 11, articolo 52, paragrafo 1, della Carta, non osta a misure legislative

<sup>36</sup> Punto 47 delle sue osservazioni scritte. Valutazione sulla quale hanno insistito anche alcuni governi in udienza.

<sup>37</sup> Groupe Échange d'informations et protection des données (DAPIX). Dello stesso parere si è dichiarato il governo svedese al punto 21 delle sue osservazioni scritte.

<sup>38</sup> Al paragrafo 92 delle conclusioni *Ordre des barreaux francophones et germanophone* ho rilevato che detti gruppi di lavoro hanno preso in considerazione, come vie da esplorare, la limitazione delle categorie di dati conservati, la pseudonimizzazione dei dati, la fissazione di periodi di conservazione limitati, l'esclusione di determinate categorie di fornitori di servizi di comunicazione elettronica, le autorizzazioni alla conservazione rinnovabili, l'obbligo di conservare i dati memorizzati nell'Unione o il controllo sistematico e costante da parte di un'autorità amministrativa indipendente delle garanzie offerte dai fornitori di servizi di comunicazione elettronica contro l'uso indebito dei dati.

<sup>39</sup> Conclusioni *Ordre des barreaux francophones et germanophone*, paragrafi 93 e 94.

<sup>40</sup> *Ibidem*, paragrafo 95.

<sup>41</sup> *Ibidem*, paragrafo 104.

- che consentano, a fini di salvaguardia della sicurezza nazionale, il ricorso a un’ingiunzione che imponga ai fornitori di servizi di comunicazione elettronica di procedere a una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all’ubicazione, in situazioni nelle quali lo Stato membro interessato affronti una minaccia grave per la sicurezza nazionale che risulti reale e attuale o prevedibile, e il provvedimento che prevede tale ingiunzione possa essere oggetto di un controllo effettivo, da parte di un giudice o di un organo amministrativo indipendente, la cui decisione sia dotata di effetto vincolante, diretto ad accertare l’esistenza di una di tali situazioni nonché il rispetto delle condizioni e delle garanzie che devono essere previste, e detta ingiunzione possa essere emessa solo per un periodo temporalmente limitato allo stretto necessario, ma sia rinnovabile in caso di persistenza di tale minaccia;
- che prevedano, a fini di salvaguardia della sicurezza nazionale, di lotta alle forme gravi di criminalità e di prevenzione delle minacce gravi alla sicurezza pubblica, una conservazione mirata dei dati relativi al traffico e dei dati relativi all’ubicazione che sia delimitata, sulla base di elementi oggettivi e non discriminatori, in funzione delle categorie di persone interessate o mediante un criterio geografico, per un periodo temporalmente limitato allo stretto necessario, ma rinnovabile;
- che prevedano, a fini di salvaguardia della sicurezza nazionale, di lotta alle forme gravi di criminalità e di prevenzione delle minacce gravi alla sicurezza pubblica, la conservazione generalizzata e indifferenziata degli indirizzi IP attribuiti all’origine di una connessione, per un periodo temporalmente limitato allo stretto necessario;
- che prevedano, a fini di salvaguardia della sicurezza nazionale, di lotta alla criminalità e di salvaguardia della sicurezza pubblica, una conservazione generalizzata e indifferenziata dei dati relativi all’identità civile degli utenti di mezzi di comunicazione elettronica, e
- che consentano, a fini di lotta alle forme gravi di criminalità e, a fortiori, di salvaguardia della sicurezza nazionale, il ricorso a un’ingiunzione che imponga ai fornitori di servizi di comunicazione elettronica, mediante un provvedimento dell’autorità competente soggetto a un controllo giurisdizionale effettivo, di procedere, per un periodo determinato, alla conservazione rapida dei dati relativi al traffico e dei dati relativi all’ubicazione di cui detti fornitori di servizi dispongono,

se tali misure garantiscono, mediante norme chiare e precise, che la conservazione dei dati di cui trattasi sia subordinata al rispetto delle relative condizioni sostanziali e procedurali e che le persone interessate dispongano di garanzie effettive contro il rischio di abusi».

### ***E. Valutazione della normativa oggetto dei presenti rinvii pregiudiziali, alla luce della sentenza La Quadrature du Net***

53. Secondo il giudice del rinvio, cui spetta in via esclusiva l’interpretazione della legislazione tedesca, quest’ultima richiede «la conservazione, senza alcuna motivazione, generalizzata e senza distinzioni personali, temporali e geografiche, di gran parte dei dati relativi al traffico delle telecomunicazioni rilevanti»<sup>42</sup>.

<sup>42</sup> Punto 25b, lettera b), della versione originale in lingua tedesca della decisione di rinvio.

54. La normativa nazionale controversa non si limita ad autorizzare le autorità competenti a richiedere la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione per un periodo limitato: è il legislatore ad imporre direttamente, e in maniera indefinita, l'obbligo di conservarli.

55. Ciò premesso, detto giudice ha elencato, nella sua comunicazione del 13 gennaio 2021, le differenze tra le norme nazionali e quelle considerate nella sentenza *La Quadrature du Net*, differenze che potrebbero condurre a una soluzione diversa da quella adottata in detta sentenza.

56. Esaminerò le suddette differenze nello stesso ordine in cui le presenta il giudice del rinvio, ma devo prima riconoscere che il legislatore tedesco ha assolto con cura il compito di adeguare la normativa nazionale ai requisiti derivanti, in tale ambito, dalla giurisprudenza della Corte.

57. Come rilevato dal giudice del rinvio, la normativa controversa è il risultato di una modifica legislativa indotta dalla giurisprudenza del *Bundesverfassungsgericht* (Corte costituzionale federale) e dagli effetti della dottrina elaborata nella sentenza *Digital Rights*.

58. Sono quindi encomiabili i progressi della legislazione nazionale in questione, derivanti da una forte volontà di adeguamento alla giurisprudenza della Corte.

59. Tuttavia, lo sforzo normativo ha forse posto l'accento più sugli aspetti relativi alla tutela e all'accesso ai dati conservati, ma meno su quelli relativi alla delimitazione mirata dei dati di cui è imposta la conservazione.

### *1. Tipologia dei dati conservati*

60. La tipologia dei dati conservati (non vengono memorizzati quelli relativi ai siti Internet consultati, quelli della posta elettronica e quelli inerenti alle comunicazioni da e verso servizi di assistenza telefonica di carattere sociale o religioso) non impedisce, a mio avviso, di ignorare che l'obbligo di conservazione generalizzata e indifferenziata si estende a un insieme molto ampio di numerosi altri dati relativi al traffico e all'ubicazione, analogo, nel complesso, a quello esaminato nella sentenza *La Quadrature du Net*.

61. A tale proposito, è quasi irrilevante, date le loro caratteristiche particolari e la loro scarsa incidenza sul computo globale<sup>43</sup>, il fatto che siano esclusi i dati relativi alle comunicazioni verso determinate linee di assistenza telefonica fornita da persone, autorità o organizzazioni in ambiti sociali o religiosi.

62. Non è determinate neppure il fatto che l'obbligo di conservazione non si estenda ai contenuti (dei siti consultati su Internet o della posta elettronica), dato che la sentenza *La Quadrature du Net* non si riferiva ad essi, bensì ai dati relativi al traffico e ai dati relativi all'ubicazione delle comunicazioni elettroniche.

<sup>43</sup> In udienza, il governo tedesco ha quantificato in 1 300 il numero degli enti le cui comunicazioni elettroniche sono escluse dall'obbligo di conservazione e ha chiarito che l'esclusione non è applicabile ai professionisti soggetti a obblighi di segretezza professionale (come gli avvocati o i medici), dato il loro numero elevato.

## 2. Durata dell'obbligo di conservazione dei dati

63. La differenza più significativa rispetto alle norme nazionali esaminate nella sentenza *La Quadrature du Net* riguarda la durata della conservazione che, secondo l'articolo 113b, paragrafo 1, del TKG, è di quattro o dieci settimane (quattro settimane nel caso dei dati relativi all'ubicazione e dieci settimane per gli altri), anziché di un anno.

64. Sia il giudice del rinvio che alcuni governi intervenuti insistono su tale circostanza, sottolineando che la normativa controversa riduce sensibilmente il periodo di conservazione dei dati. Secondo il giudice del rinvio, la minore durata riduce il rischio che si possa tracciare un profilo complessivo delle persone interessate.

65. Come ho sostenuto nelle conclusioni *Ordre des barreaux francophones et germanophone*, riferendomi proprio alla normativa nazionale ora in esame, i dati memorizzati devono poter essere conservati solo per un periodo limitato<sup>44</sup>, in funzione della loro appartenenza a una categoria o a un'altra<sup>45</sup>.

66. Tuttavia, se pure la limitazione temporale del periodo di conservazione è un elemento rilevante al fine di valutare la normativa controversa, tale circostanza non può compensare il fatto che essa impone una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione.

67. Ho già rilevato che, secondo la giurisprudenza della Corte, al di fuori dell'ipotesi giustificata dalla difesa della sicurezza nazionale, è possibile solo una conservazione mirata dei dati relativi alle comunicazioni elettroniche, considerati i gravi rischi che comporterebbe la loro conservazione generalizzata.

68. Tale rischio è stato, in definitiva, quello che ha ispirato la giurisprudenza della Corte in materia: «i dati relativi al traffico e i dati relativi all'ubicazione possono rivelare informazioni su un numero significativo di aspetti della vita privata degli interessati, comprese informazioni sensibili, quali l'orientamento sessuale, le opinioni politiche, le convinzioni religiose, filosofiche, sociali o di altro tipo nonché lo stato di salute, mentre tali dati beneficiano, peraltro, di una tutela particolare nel diritto dell'Unione. Presi nel loro insieme, tali dati sono idonei a consentire di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini della vita quotidiana, i luoghi di soggiorno permanenti o temporanei, gli spostamenti giornalieri o di altro tipo, le attività esercitate, le relazioni sociali di dette persone e gli ambienti sociali da esse frequentati. In particolare, questi dati forniscono gli strumenti per stabilire il profilo delle persone interessate, informazione tanto sensibile, in rapporto al diritto al rispetto della vita privata, quanto il contenuto stesso delle comunicazioni»<sup>46</sup>.

69. È vero che, come afferma il giudice del rinvio, una conservazione molto limitata nel tempo può rendere più difficile la profilazione.

<sup>44</sup> Conclusioni *Ordre des barreaux francophones et germanophone*, paragrafo 96. Si evita in tale modo che essi «consentano di offrire un'immagine dettagliata della vita delle persone interessate. Tale periodo di conservazione deve inoltre essere adattato in funzione della natura dei dati, così che quelli che forniscono informazioni più precise sullo stile di vita e le abitudini di dette persone siano conservati per un periodo di tempo più breve».

<sup>45</sup> *Ibidem*, paragrafo 97. «In altri termini, la diversificazione del periodo di conservazione di ciascuna categoria di dati, in funzione della sua utilità per conseguire gli obiettivi di sicurezza, è una strada che deve essere esplorata. Riducendo il periodo in cui le varie categorie di dati sono conservate simultaneamente (e, pertanto, possono essere utilizzate per trovare correlazioni che rivelino lo stile di vita delle persone interessate), si estende la protezione del diritto tutelato dall'articolo 8 della Carta».

<sup>46</sup> Sentenza *La Quadrature du Net*, punto 117.

70. Tuttavia, la maggiore o minore difficoltà a tale riguardo non dipende solo dal tempo di conservazione, ma anche dalla quantità e qualità dei dati conservati: quanto più è elevato il numero di dati, tanto più si potranno ottenere informazioni sensibili per periodi di tempo la cui estensione dipenderà, a sua volta, dall'evoluzione delle tecniche di controllo, correlazione e valutazione del complesso dei dati relativi alle comunicazioni elettroniche. Quello che oggi può risultare un tempo insufficiente per accumulare informazioni che consentano la profilazione potrebbe essere più che sufficiente per riuscirvi in un futuro più o meno prossimo<sup>47</sup>.

71. Ad ogni modo, secondo la Corte, «l'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta, derivante dall'accesso, da parte di un'autorità pubblica, a un insieme di dati relativi al traffico o di dati relativi all'ubicazione, suscettibili di fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali da esso utilizzate, presenta in ogni caso un carattere grave *indipendentemente dalla durata del periodo per il quale è richiesto l'accesso a tali dati* e dalla quantità o dalla natura dei dati disponibili per un periodo siffatto, qualora (...) questo insieme di dati sia tale da permettere di trarre precise conclusioni sulla vita privata della persona o delle persone interessate»<sup>48</sup>.

72. In definitiva, ritengo che, nonostante le differenze segnalate dal giudice del rinvio, le analogie su tale aspetto tra la normativa di cui trattasi nei procedimenti principali e le legislazioni oggetto dei procedimenti che hanno dato luogo alla sentenza *La Quadrature du Net* non consentano di discostarsi dalla giurisprudenza di quest'ultima.

### 3. Protezione dei dati contro l'accesso illecito

73. Le norme tedesche, secondo il giudice del rinvio, offrono una protezione efficace dei dati conservati contro i pericoli di abuso e di accesso illecito.

74. Senza svilire lo sforzo normativo per quanto riguarda la protezione e l'accesso ai dati, non si deve dimenticare che, secondo la Corte, «la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione costituisce, *di per sé*, (...) un'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali»<sup>49</sup>. In tal senso, «l'accesso a tali dati costituisce, a prescindere dall'uso che ne viene fatto in seguito, un'*ingerenza distinta*» nei menzionati diritti fondamentali<sup>50</sup>.

75. È quindi irrilevante, per quanto interessa in questa sede, che il regime di protezione dei dati conservati previsto dal legislatore tedesco: a) garantisca effettivamente l'indennità di tali dati, b) delimiti le condizioni di accesso in modo rigoroso ed efficace, circoscrivendo la cerchia dei soggetti che possono accedervi, e c) consenta l'utilizzo dei dati conservati solo a fini di indagine su reati gravi e per la prevenzione di rischi concreti per la vita o la libertà delle persone o la sicurezza dello Stato.

<sup>47</sup> Come è emerso in udienza, anche un periodo di dieci settimane di raccolta di metadati (dati relativi al traffico e dati relativi all'ubicazione) potrebbe essere sufficiente per identificare le modalità di comportamento dell'abbonato che, con la loro ricorrenza, rivelino caratteristiche sensibili della sua personalità e della sua vita.

<sup>48</sup> Sentenza del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche) (C-746/18, EU:C:2021:152, punto 39). Il corsivo è mio.

<sup>49</sup> Sentenza *La Quadrature du Net*, punto 115.

<sup>50</sup> *Ibidem*, punto 116. Il corsivo è mio.

76. L'elemento realmente decisivo è che, come ripete anche il giudice del rinvio, l'obbligo di conservazione di cui trattasi, di per sé, non è soggetto ad alcuna condizione specifica.

#### *4. Incidenza della sentenza del Bundesverfassungsgericht (Corte costituzionale federale) del 27 maggio 2020*

77. Il giudice del rinvio fa riferimento a una pronuncia del Bundesverfassungsgericht (Corte costituzionale federale) sull'articolo 113 del TKG<sup>51</sup>, per effetto della quale la validità di tale disposizione, dopo la relativa declaratoria di incostituzionalità, sarebbe stata subordinata a condizioni la cui compatibilità con il diritto dell'Unione non sarebbe facile da determinare.

78. La Corte non ha nulla da dire, in questa fase, sugli effetti di detta sentenza né tanto meno sui contorni delle nuove norme che il legislatore tedesco deve adottare (o ha adottato, a seconda dei casi).

79. Se, come afferma il giudice del rinvio, esso deve basare la sua sentenza di «Revision» sulla normativa vigente alla data in cui si pronuncia, il medesimo dovrà statuire autonomamente in merito alla compatibilità di detta normativa con il diritto dell'Unione alla luce della giurisprudenza della Corte in materia di protezione dei dati delle comunicazioni elettroniche.

#### *5. Indirizzi IP*

80. Secondo il giudice del rinvio, dal punto 168 della sentenza *La Quadrature du Net* risulterebbe che la Corte richiede per gli indirizzi IP un motivo di conservazione connesso all'obiettivo di salvaguardia della sicurezza nazionale, di lotta contro le forme gravi di criminalità e di prevenzione delle minacce gravi alla sicurezza pubblica. Tuttavia, dal punto 155 si evincerebbe che tali indirizzi IP possono essere conservati senza necessità di una motivazione specifica, in quanto occorrerebbe un motivo connesso a detto obiettivo soltanto per l'utilizzo dei dati conservati.

81. Tuttavia, non ritengo che sussista detta conflittualità (né tanto meno una contraddizione). Sebbene al punto 155 la Corte affermi che la conservazione generalizzata e indifferenziata degli indirizzi IP attribuiti all'origine di una connessione «non risulta, in linea di principio, contraria all'articolo 15, paragrafo 1, della direttiva 2002/58», più avanti essa dichiara, al punto 156, che, «[t]enuto conto della gravità dell'ingerenza nei diritti fondamentali (...) che tale conservazione comporta, solo la lotta alle forme gravi di criminalità e la prevenzione delle minacce gravi alla sicurezza pubblica sono idonee, al pari della salvaguardia della sicurezza nazionale, a giustificare siffatta ingerenza. (...)».

82. Dal combinato dei punti 155 e 156 della sentenza *La Quadrature du Net* deriva quindi la risposta coerente che, al punto 168, la Corte ha fornito alle questioni pregiudiziali allora sollevate riguardo alla conservazione degli indirizzi IP.

83. In udienza sono stati evidenziati taluni problemi – che, ad avviso di alcuni intervenienti, richiederebbero un chiarimento da parte della Corte – relativi alla conservazione degli indirizzi IP. La soluzione di tali problemi (tra l'altro, quelli determinati dalla differenza tra gli indirizzi IP

<sup>51</sup> V. nota 19 delle presenti conclusioni.

dinamici e quelli statici, nonché l'incidenza del protocollo Ipv6) esula, a mio parere, dalle questioni del giudice del rinvio, le cui domande di pronuncia pregiudiziale iniziali<sup>52</sup> e la cui comunicazione del 13 gennaio 2021 hanno, su questo punto, una portata molto più limitata.

## V. Conclusione

84. In considerazione di quanto precede, suggerisco alla Corte di rispondere al Bundesverwaltungsgericht (Corte amministrativa federale, Germania) nei termini seguenti:

«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 e 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea e dell'articolo 4, paragrafo 2, TUE, deve essere interpretato nel senso che esso osta ad una normativa nazionale la quale imponga ai fornitori di servizi di comunicazione elettronica accessibili al pubblico di conservare, in modo preventivo, generale e indifferenziato, i dati relativi al traffico e i dati relativi all'ubicazione degli utenti finali di detti servizi per finalità diverse dalla salvaguardia della sicurezza nazionale di fronte a una minaccia che risulti reale e attuale o prevedibile».

<sup>52</sup> Punto 30 della decisione di rinvio.