

Edizione provvisoria

CONCLUSIONI DELL'AVVOCATO GENERALE  
MACIEJ SZPUNAR  
presentate il 3 settembre 2026 ([1](#))

**Causa C-661/24**

**Ordre des barreaux francophones et germanophone,  
Académie Fiscale ASBL,  
UA,  
vzw Liga voor Mensenrechten,  
Ligue des droits humains ASBL,  
JU,  
LV,  
Ministry of Privacy  
contro  
Premier ministre/ Eerste Minister**

[domanda di pronuncia pregiudiziale proposta dalla Cour constitutionnelle (Corte costituzionale, Belgio)]

« Rinvio pregiudiziale – Settore delle telecomunicazioni – Trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche – Direttiva 2002/58/CE – Facoltà per gli Stati membri di adottare misure di conservazione dei dati per la prevenzione, la ricerca, l'accertamento e il perseguimento dell'uso non autorizzato del sistema di comunicazione elettronica »

## **I. Introduzione**

1. Con l'adozione della legge del 20 luglio 2022 relativa alla raccolta e alla conservazione dei dati identificativi e dei metadati nel settore delle comunicazioni

elettroniche e alla fornitura di tali dati alle autorità (in prosieguo: la «legge del 20 luglio 2022»), il legislatore belga ha inteso rendere la normativa nazionale conforme alla sentenza della Cour constitutionnelle (Corte costituzionale, Belgio) che annulla la legge del 29 maggio 2016 relativa alla raccolta e alla conservazione dei dati nel settore delle comunicazioni elettroniche (2).

2. Tale sentenza era stata pronunciata a seguito della sentenza della Corte, la *Quadrature du Net e a.* (3), relativa all'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58/CE(4), letto alla luce degli articoli 7, 9 e 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»).

3. Investita di cinque ricorsi diretti all'annullamento totale o parziale della legge del 20 luglio 2022, la Cour constitutionnelle interroga nuovamente la Corte sull'interpretazione di tali disposizioni, relativamente alla nuova normativa nazionale che consente, in particolare, la conservazione di un certo numero di dati relativi al traffico e all'ubicazione.

4. La presente causa offre quindi alla Corte l'opportunità di precisare la propria giurisprudenza già fornita in materia, in particolare per quanto riguarda la portata degli ultimi sviluppi ad essa relativi derivanti dalla sentenza *Quadrature du Net e a.* [\(Dati personali e lotta alla contraffazione\)](#) (5).

## II. Contesto normativo

### A. Diritto dell'Unione

5. I considerando 2, 6, 7, 11, 14, 15, 20, 22, 26, 29, 30, 35 e 36 della direttiva 2002/58 enunciano quanto segue:

«(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 tale Carta.

(...)

(6) L'Internet ha sconvolto le tradizionali strutture del mercato fornendo un'infrastruttura mondiale comune per la fornitura di un'ampia serie di servizi di comunicazione elettronica. I servizi di comunicazione elettronica accessibili al pubblico attraverso l'Internet aprono nuove possibilità agli utenti ma rappresentano anche nuovi pericoli per i loro dati personali e la loro vita privata.

(7) Nel settore delle reti pubbliche di comunicazione occorre adottare disposizioni legislative, regolamentari e tecniche specificamente finalizzate a tutelare i diritti e le libertà fondamentali delle persone fisiche e i legittimi interessi delle persone giuridiche, con particolare riferimento all'accresciuta capacità di memorizzazione e trattamento dei dati relativi agli abbonati e agli utenti.

(...)

(11) La presente direttiva, analogamente alla direttiva 95/46/CE[(6) ], non affronta le questioni relative alla tutela dei diritti e delle libertà fondamentali inerenti ad attività che non sono disciplinate dal diritto [dell'Unione]. 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, [firmata a Roma il 4 novembre 1950, (in prosieguo: la "CEDU"),] come interpretata dalle sentenze della Corte europea dei diritti dell'uomo [(in prosieguo: la "Corte EDU")]. Tali misure devono essere appropriate, strettamente proporzionate allo scopo perseguito, necessarie in una società democratica ed essere soggette ad idonee garanzie conformemente alla precitata [CEDU].

(...)

(14) I dati relativi all'ubicazione possono riferirsi alla latitudine, longitudine ed altitudine dell'apparecchio terminale dell'utente, alla direzione di viaggio, al livello di accuratezza dell'informazione sull'ubicazione, all'identificazione della cella di rete in cui l'apparecchio terminale è ubicato in un determinato momento, e al momento in cui l'informazione sull'ubicazione è stata registrata.

(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. I dati relativi al traffico possono tra l'altro consistere in dati che si riferiscono all'instradamento, alla durata, al tempo o al volume di una comunicazione, al protocollo usato, all'ubicazione dell'apparecchio terminale di chi invia o riceve, alla rete sulla quale la comunicazione si origina o termina, all'inizio, alla fine o alla durata di un collegamento. Possono anche consistere nel formato in cui la comunicazione è trasmessa dalla rete.

(...)

(20) I fornitori di servizi dovrebbero adottare misure appropriate per salvaguardare la sicurezza dei servizi da essi offerti, se necessario congiuntamente al fornitore della rete, e dovrebbero informare gli abbonati sui particolari rischi di violazione della sicurezza della rete. Tali rischi possono presentarsi segnatamente per i servizi di comunicazione elettronica su una rete aperta come l'Internet o la telefonia mobile analogica. È di

particolare importanza per gli utenti e gli abbonati di tali servizi essere pienamente informati dal loro fornitore di servizi dell'esistenza di rischi alla sicurezza al di fuori della portata dei possibili rimedi esperibili dal fornitore stesso. I fornitori di servizi che offrono servizi di comunicazione elettronica accessibili al pubblico su Internet dovrebbero informare gli utenti e gli abbonati delle misure che questi ultimi possono prendere per proteggere la sicurezza delle loro comunicazioni, ad esempio attraverso l'uso di particolari tipi di programmi o tecniche di criptaggio. L'obbligo di informare gli abbonati su particolari rischi relativi alla sicurezza non esonera il fornitore di servizi dall'obbligo di prendere, a sue proprie spese, provvedimenti adeguati ed immediati per rimediare a tutti i nuovi, imprevisti rischi relativi alla sicurezza e ristabilire il normale livello di sicurezza del servizio. La fornitura all'abbonato di informazioni sui rischi relativi alla sicurezza dovrebbe essere gratuita fatta eccezione per i costi nominali che l'abbonato può sostenere quando riceve o prende conoscenza delle informazioni, per esempio scaricando un messaggio di posta elettronica. La sicurezza viene valutata alla luce dell'articolo 17 della direttiva [95/46].

(...)

(22) Il divieto di memorizzare comunicazioni e i relativi dati sul traffico da parte di persone diverse dagli utenti o senza il loro consenso non è inteso a vietare eventuali memorizzazioni automatiche, intermedie e temporanee di tali informazioni fintanto che ciò viene fatto unicamente a scopo di trasmissione nella rete di comunicazione elettronica e a condizione che l'informazione non sia memorizzata per un periodo superiore a quanto necessario per la trasmissione e ai fini della gestione del traffico e che durante il periodo di memorizzazione sia assicurata la riservatezza dell'informazione.

(...)

(...)

(26) I dati relativi agli abbonati sottoposti a trattamento nell'ambito di reti di comunicazione elettronica per stabilire i collegamenti e per trasmettere informazioni contengono informazioni sulla vita privata delle persone fisiche e riguardano il diritto al rispetto della loro corrispondenza o i legittimi interessi delle persone giuridiche. Tali dati possono essere memorizzati solo nella misura necessaria per la fornitura del servizio ai fini della fatturazione e del pagamento per l'interconnessione, nonché per un periodo di tempo limitato. Qualsiasi ulteriore trattamento di tali dati (...) può essere autorizzato soltanto se l'abbonato abbia espresso il proprio consenso in base ad informazioni esaurienti ed accurate date dal fornitore dei servizi di comunicazione elettronica accessibili al pubblico circa la natura dei successivi trattamenti che egli intende effettuare e circa il diritto dell'abbonato di non dare o di revocare il proprio consenso a tale trattamento. I dati relativi al traffico utilizzati per la commercializzazione dei servizi di comunicazione (...) dovrebbero inoltre essere cancellati o resi anonimi (...)

(...)

(29) Il fornitore di servizi può trattare i dati sul traffico relativi agli abbonati ed agli utenti ove necessario in singoli casi per individuare problemi tecnici od errori materiali nella trasmissione delle comunicazioni. I dati relativi al traffico necessari ai fini della fatturazione possono anche essere sottoposti a trattamento da parte del fornitore per accertare e sospendere la frode che consiste nell'uso del servizio di comunicazione elettronica senza il corrispondente pagamento.

(30) I sistemi per la fornitura di reti e servizi di comunicazione elettronica dovrebbero essere progettati per limitare al minimo la quantità di dati personali necessari (...)

(...)

(35) Nelle reti mobili digitali i dati relativi all'ubicazione, che consentono di determinare la posizione geografica dell'apparecchiatura terminale dell'utente mobile vengono sottoposti a trattamento in modo da consentire la trasmissione di comunicazioni. Tali dati sono quelli relativi al traffico di cui all'articolo 6 della presente direttiva. Tuttavia, in aggiunta ad essi, le reti mobili digitali possono avere la capacità di trattare dati relativi all'ubicazione che possiedono un grado di precisione molto maggiore di quello necessario per la trasmissione delle comunicazioni e che vengono utilizzati per fornire servizi a valore aggiunto, come i servizi che forniscono informazioni individuali sul traffico e radioguida. Il trattamento di dati siffatti ai fini della fornitura di servizi a valore aggiunto dovrebbe essere autorizzato soltanto previo esplicito consenso dell'abbonato. Anche in questo caso, tuttavia, gli abbonati dovrebbero disporre, gratuitamente, di un mezzo semplice per bloccare temporaneamente il trattamento dei dati relativi alla loro ubicazione.

(36) Gli Stati membri possono limitare il diritto alla vita privata degli utenti e degli abbonati riguardo all'identificazione della linea chiamante allorché ciò sia necessario per identificare le chiamate importune, e riguardo all'identificazione della linea chiamante e ai dati relativi all'ubicazione allorché ciò sia necessario per consentire ai servizi di emergenza di svolgere il loro compito nel modo più efficace possibile. A tale scopo gli Stati membri possono adottare disposizioni specifiche per autorizzare i fornitori di servizi di comunicazione elettronica a fornire l'accesso all'identificazione della linea chiamante e ai dati relativi all'ubicazione senza il previo consenso degli utenti o abbonati interessati».

6. L'articolo 1, paragrafo 1, di tale direttiva, intitolato «Finalità e campo d'applicazione», così dispone:

«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 dell'[Unione europea]».

7. L'articolo 2 di detta direttiva, intitolato «Definizioni», così recita:

«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)[(Z)].

Si applicano inoltre le seguenti definizioni:

- a) “utente”: qualsiasi persona fisica che utilizzi un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;
- 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. A termini dell’articolo 5 della medesima direttiva, intitolato «Riservatezza delle comunicazioni»:

«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.

(...)

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.

Ciò non vieta l'eventuale archiviazione tecnica o l'accesso al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio».

9. 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.

3. Ai fini della commercializzazione dei servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha facoltà di sottoporre a trattamento i dati di cui al paragrafo 1 nella misura e per la durata necessaria per siffatti servizi, o per la commercializzazione, sempre che l'abbonato o l'utente a cui i dati si riferiscono abbia espresso preliminarmente il proprio consenso. Gli abbonati o utenti hanno la possibilità di ritirare il loro consenso al trattamento dei dati relativi al traffico in qualsiasi momento.

(...)

5. Il trattamento dei dati relativi al traffico ai sensi dei paragrafi da 1 a 4 deve essere limitato alle persone che agiscono sotto l'autorità dei fornitori della rete pubblica di comunicazione elettronica e dei servizi di comunicazione elettronica accessibili al pubblico che si occupano della fatturazione o della gestione del traffico, delle indagini per conto dei clienti, dell'accertamento delle frodi, della commercializzazione dei servizi di comunicazione elettronica o della prestazione di servizi a valore aggiunto. Il trattamento deve essere limitato a quanto è strettamente necessario per lo svolgimento di tali attività

(...)».

10. L'articolo 9 di tale direttiva, intitolato «Dati relativi all'ubicazione diversi dai dati relativi al traffico», prevede, al paragrafo 1, quanto segue:

«Se i dati relativi all'ubicazione diversi dai dati relativi al traffico, relativi agli utenti o abbonati di reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico possono essere sottoposti a trattamento, essi possono esserlo

soltanto a condizione che siano stati resi anonimi o che l'utente o l'abbonato abbiano dato il loro consenso, e sempre nella misura e per la durata necessaria per la fornitura di un servizio a valore aggiunto. Prima di chiedere il loro consenso, il fornitore del servizio deve informare gli utenti e gli abbonati sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti a trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto (...).

11. L'articolo 15 di detta direttiva, intitolato «Applicazione di alcune disposizioni della direttiva [95/46]», stabilisce quanto segue:

«1. 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 [dell'Unione], compresi quelli di cui all'articolo 6, paragrafi 1 e 2, [TUE].

(...)

2. Le disposizioni del capo III della direttiva [95/46] relative ai ricorsi giurisdizionali, alle responsabilità e alle sanzioni si applicano relativamente alle disposizioni nazionali adottate in base alla presente direttiva e con riguardo ai diritti individuali risultanti dalla stessa.

(...)».

## B. **Diritto belga**

12. La legge del 20 luglio 2022 ha modificato, tra l'altro, la legge del 17 gennaio 2003 relativa allo status dell'organismo belga di vigilanza sui settori delle poste e telecomunicazioni (in prosieguo: la «legge del 17 gennaio 2003») nonché la legge del 13 giugno 2005 relativa alle comunicazioni elettroniche (in prosieguo: la «legge del 13 giugno 2005»).

### 1. **Legge del 17 gennaio 2003**

13. L'articolo 25/1 della legge del 17 gennaio 2003, come modificato dall'articolo 24 della legge del 20 luglio 2022, è così formulato:

§ 1. Al fine di ricercare, accertare o perseguire un reato di cui all'articolo 145, § 3 o § 3bis, della [legge del 13 giugno 2005] o all'articolo 24, § 1, punto 2, un ufficiale di polizia giudiziaria dell'[Institut belge des services postaux et des télécommunications (Istituto belga dei servizi postali e delle telecomunicazioni; in prosieguo: l'«Istituto»)] può, per iscritto:

- 1° imporre a un operatore di rispondere a una richiesta di dati identificativi necessaria a tali fini;
- 2° chiedere la collaborazione delle persone e delle istituzioni di cui all'articolo 46<sup>quater</sup>, § 1, del Code d'instruction criminelle (codice di procedura penale) e di associazioni che le rappresentano, sulla base del riferimento di pagamento online specifico di un servizio di comunicazione elettronica precedentemente comunicato da un operatore conformemente al punto 1°, al fine di identificare la persona che ha pagato il servizio;
- 3° chiedere la collaborazione dei centri chiusi o delle strutture ricettive ai sensi degli articoli 74/8 e 74/9 della legge del 15 dicembre 1980 in materia di ingresso nel territorio, soggiorno, insediamento e allontanamento degli stranieri, presso cui sia stata effettuata la sottoscrizione da parte dell'abbonato di un servizio di comunicazione elettronica, sulla base delle coordinate del centro o della struttura ricettiva precedentemente comunicate da un operatore conformemente al punto 1° al fine di identificare l'abbonato;
- 4° chiedere la collaborazione di qualsiasi altra persona giuridica che sia l'abbonato di un operatore o che sottoscriva un servizio di comunicazione elettronica in nome e per conto di persone fisiche, sulla base dei dati precedentemente comunicati da un operatore conformemente al punto 1°, al fine di identificare l'utente abituale del servizio.

La richiesta di cui al comma 1 può essere trasmessa ad un attore di cui al comma 1 solo previa autorizzazione scritta di un ufficiale di polizia giudiziaria di cui all'articolo 24, § 2. Tale autorizzazione può essere concessa solo su richiesta scritta e motivata indirizzata a detto ufficiale conformemente al paragrafo 5.

§ 2. Per le esigenze connesse all'esecuzione dei suoi compiti, un ufficiale di polizia giudiziaria dell'Istituto può imporre a un operatore, per iscritto, di rispondere a una richiesta di metadati necessaria al fine di ricercare, accertare o perseguire un reato di cui all'articolo 145, § 3 o § 3bis, della [legge del 13 giugno 2005], o all'articolo 24, § 1, punto 2°.

Salvo i casi di urgenza debitamente giustificata, l'ufficiale di polizia giudiziaria dell'Istituto può indirizzare la richiesta all'operatore solo dopo aver presentato una domanda scritta e motivata al giudice istruttore e previa autorizzazione scritta di quest'ultimo.

In caso di urgenza debitamente giustificata menzionata al comma 2, l'ufficiale di polizia giudiziaria dell'Istituto trasmette senza indugio al giudice istruttore, dopo l'invio della richiesta all'operatore, una copia di tale richiesta, con la motivazione della stessa e la giustificazione dell'urgenza. Il giudice istruttore effettua un ulteriore controllo.

Qualora, a seguito di tale ulteriore controllo, il giudice istruttore rifiuti di convalidare la richiesta inviata dall'ufficiale di polizia giudiziaria dell'Istituto all'operatore, detto ufficiale ne dà senza indugio notifica all'operatore interessato e cancella i metadati ricevuti.

§ 3. In deroga ai paragrafi 1 e 2, al fine di verificare l'osservanza degli articoli 126, 126/1, 126/2, 126/3 o 127 [legge del 13 giugno 2005], e dei relativi decreti esecutivi e su richiesta scritta e motivata di un ufficiale di polizia giudiziaria dell'Istituto, un operatore fornisce, entro il termine fissato nella requisitoria, un accesso che consenta di consultare le sue banche dati che attuano uno di tali articoli o uno di tali decreti esecutivi.

La richiesta di cui al comma 1 può essere trasmessa a un operatore solo previa autorizzazione scritta di un ufficiale di polizia giudiziaria dell'Istituto di cui all'articolo 24, § 2. Tale autorizzazione può essere concessa solo su richiesta scritta e motivata a norma del paragrafo 5.

La richiesta indirizzata all'operatore precisa i nomi degli ufficiali di polizia giudiziaria dell'Istituto che possono consultare la banca dati.

Tali ufficiali possono fare una copia dei dati e dei documenti consultati nell'ambito del comma 1 soltanto allo scopo di accertare reati commessi dall'operatore.

§ 4. Ai fini dell'applicazione dei paragrafi 1 e 2, gli attori di cui al paragrafo 1, comma 1, ai quali un ufficiale di polizia giudiziaria dell'Istituto ha chiesto dati, gli trasmettono tali dati in tempo reale o, se del caso, al momento precisato nella requisitoria.

Ai fini dell'applicazione dei paragrafi da 1 a 3, chiunque, in ragione delle sue funzioni, abbia conoscenza del provvedimento o vi abbia concorso, è tenuto al segreto. Le violazioni del segreto sono punite secondo quanto previsto dall'articolo 458 del codice penale.

Chiunque rifiuti di comunicare i dati o non li comunichi in tempo reale o, se del caso, al momento precisato nella requisitoria è punito con una sanzione pecuniaria da EUR 26 a EUR 10 mila.

Chiunque rifiuti di consentire la consultazione della banca dati conformemente al paragrafo 3 o che non consenta tale consultazione entro il termine fissato nella requisitoria è punito con una sanzione pecuniaria da EUR 26 a EUR 10 mila.

§ 5. Ai fini dell'applicazione dei paragrafi da 1 a 3, la motivazione della domanda indirizzata all'ufficiale di polizia giudiziaria di cui all'articolo 24, § 2, o al giudice istruttore deve essere elaborata alla luce delle circostanze dell'indagine.

Ai fini dell'applicazione dei paragrafi 1 e 2, tale motivazione indica:

1° il nesso tra i dati richiesti e l'obiettivo di ricerca, accertamento o perseguimento del reato specifico che giustifica la richiesta;

2° il carattere strettamente necessario dei dati richiesti nell'ambito dell'indagine.

§ 6. Gli ufficiali di polizia giudiziaria dell'Istituto inseriscono in un registro:

1° tutte le richieste di cui ai paragrafi 1, 2 e 3;

2° la motivazione della richiesta e la giustificazione dell'urgenza comunicate al giudice istruttore conformemente al paragrafo 2, comma 3;

3° le autorizzazioni di cui ai paragrafi 1, 2 e 3».

## 2. **Legge del 13 giugno 2005**

14. L'articolo 2 della legge del 13 giugno 2005, come modificato dalla legge del 20 luglio 2022, così prevede:

«Ai fini dell'applicazione della presente legge, si deve intendere per:

(...)

5/5° "frode": un atto disonesto compiuto con l'intento di ingannare in violazione di leggi, regolamenti o contratti o di procurare a sé o ad altri un vantaggio illecito a danno dell'operatore o dell'utente finale mediante l'uso di un servizio di comunicazione elettronica;

5/6° "uso illecito della rete o del servizio": uso della rete o del servizio di comunicazione elettronica al fine di importunarne il corrispondente o di provocare danni;

(...)

11° "operatore": chiunque abbia presentato una notifica ai sensi dell'articolo 9;

(...)».

15. L'articolo 122 di tale legge, come modificato dall'articolo 5 della legge del 20 luglio 2022, così dispone:

«§ 1. Gli operatori cancellano i dati sul traffico relativi agli abbonati o agli utenti finali dai loro dati sul traffico o li rendono anonimi non appena non siano più necessari per la trasmissione della comunicazione.

(...)

§ 4. In deroga al paragrafo 1, al fine di poter adottare le misure appropriate di cui all'articolo 121/8, § 1, per consentire di accertare la frode o l'uso illecito della rete o del servizio o di identificarne l'autore e l'origine, e nei limiti in cui li tratta o li genera nell'ambito della fornitura di tale rete o servizio, l'operatore:

1° conserva, nell'ambito della fornitura di un servizio di comunicazioni interpersonali e per quattro mesi a decorrere dalla data della comunicazione, i dati relativi al traffico necessari a

tali fini tra i seguenti dati relativi al traffico:

- l'identificativo dell'origine della comunicazione;
- l'identificativo della destinazione della comunicazione;
- le date nonché le ore precise di inizio e fine della comunicazione;
- l'ubicazione delle apparecchiature terminali delle parti della comunicazione all'inizio e alla fine della comunicazione;

2° conserva per dodici mesi a decorrere dalla data della comunicazione i seguenti dati relativi al traffico riguardanti le comunicazioni in entrata nell'ambito della fornitura di servizi di comunicazione interpersonale al fine di identificare l'autore della comunicazione:

- il numero di telefono all'origine della comunicazione in entrata, oppure;
- l'indirizzo IP utilizzato per l'invio della comunicazione in entrata, la marcatura temporale e la porta utilizzata, e;
- le date nonché le ore precise di inizio e fine della comunicazione in entrata;

3° conserva i dati di cui al punto 1° relativi a una frode specifica accertata o a un uso illecito specifico della rete accertato per il tempo necessario alla sua analisi e alla sua soluzione, se del caso oltre il termine di quattro mesi di cui al punto 1°;

4° conserva i dati relativi al traffico di cui al punto 2° riguardanti un uso illecito specifico della rete per il tempo necessario al trattamento dello stesso, se del caso oltre il termine di dodici mesi di cui al punto 2°;

5° tratta i dati relativi al traffico necessari a tali fini, compresi, quando necessario, i dati di cui al paragrafo 2.

In deroga al paragrafo 1, al fine di poter adottare le misure appropriate di cui all'articolo 121/8, § 1, di consentire di accertare la frode o l'uso illecito della rete o del servizio o di identificarne l'autore e l'origine, l'operatore può conservare e trattare dati diversi da quelli di cui al comma 1 considerati necessari a tali fini.

La Corona può precisare ed estendere, con decreto deliberato in Consiglio dei ministri, e previo parere dell'Istituto e dell'Autorité de protection des données (Autorità per la protezione dei dati, Belgio), i dati relativi al traffico la cui conservazione deve essere considerata necessaria per perseguire gli obiettivi previsti al presente paragrafo.

In caso di frode presunta o di uso illecito presunto, gli operatori possono trasmettere alle autorità competenti tutti i dati conservati legittimamente in relazione alla frode presunta o all'uso illecito presunto.

§ 4/1. In deroga al paragrafo 1, gli operatori possono conservare e trattare i dati relativi al traffico necessari per garantire la sicurezza e il buon funzionamento delle loro reti e dei loro servizi di comunicazione elettronica, e in particolare per accertare e analizzare un attentato potenziale o reale per tale sicurezza, ivi compreso per individuare l'origine di detto attentato.

Gli operatori possono conservare tali dati per un periodo di dodici mesi a decorrere dalla data della comunicazione.

Gli operatori possono conservare i dati di cui al comma 1 relativi a un attentato specifico alla sicurezza della rete per l'arco di tempo necessario per trattarlo, se del caso oltre il termine di dodici mesi di cui al comma 2.

In caso di attentato alla sicurezza delle loro reti e dei loro servizi di comunicazione elettronica, gli operatori possono trasmettere alle autorità competenti tutti i dati conservati legittimamente in relazione all'attentato alla sicurezza delle loro reti e dei loro servizi di comunicazione elettronica».

§ 4/2. In deroga al paragrafo 1, gli operatori conservano e trattano i dati relativi al traffico necessari per adempiere un obbligo formalmente imposto da una norma legislativa, per la durata richiesta a tal fine.

§ 5. I dati elencati nel presente articolo possono essere trattati solo dalle persone incaricate dall'operatore della fatturazione o della gestione del traffico, del trattamento delle richieste di informazioni degli abbonati, della lotta contro le frodi o l'uso illecito della rete, della sicurezza della rete, del rispetto dei suoi obblighi di legge, del marketing dei propri servizi di comunicazione elettronica o della fornitura di servizi che utilizzano dati relativi al traffico o all'ubicazione e da parte dei membri della sua cellula di coordinamento di cui all'articolo 127/3.

(...)»

16. L'articolo 123 di detta legge, come modificato dall'articolo 6 della legge del 20 luglio 2022, è così formulato:

«§ 1. Fatta salva l'applicazione del [regolamento (UE) 2016/679 (8)] e della legge del 30 luglio 2018, gli operatori di reti mobili possono conservare e trattare dati relativi all'ubicazione diversi dai dati relativi al traffico riguardanti un abbonato o un utente finale esclusivamente nei seguenti casi:

1° quando sia necessario per il buon funzionamento e la sicurezza della rete o del servizio, limitando la conservazione dei dati a un massimo di dodici mesi a partire dalla data della comunicazione, salvo i casi di attentato specifico alla sicurezza della rete che necessitino di prolungare la conservazione dei dati interessati oltre tale termine;

2° quando sia necessario per accertare o analizzare le frodi o l'uso illecito della rete, limitando la conservazione dei dati a un massimo di quattro mesi a partire dalla data della

comunicazione, salvo i casi di frode o di uso illecito specifico che necessitino di prolungare la conservazione dei dati interessati oltre tale termine;

3° quando i dati siano stati resi anonimi;

4° quando il trattamento si inserisca nel quadro della fornitura di un servizio che utilizza dati relativi al traffico o all'ubicazione;

5° quando il trattamento sia necessario per adempiere un obbligo formalmente imposto a norma di legge.

(...)

§ 4. I dati di cui al presente articolo possono essere trattati solo da persone che lavorano sotto l'autorità dell'operatore o del terzo che fornisce il servizio che utilizza dati relativi al traffico o all'ubicazione o dalla cellula di coordinamento dell'operatore di cui all'articolo 127/3.

Il trattamento è limitato a quanto strettamente necessario per poter fornire al servizio in questione i dati relativi al traffico o all'ubicazione.

(...)»

### III. Procedimento principale, questioni pregiudiziali e procedimento dinanzi alla Corte

17. Le associazioni senza scopo di lucro Académie Fiscale ASBL , Ordre des barreaux francophones et germanophone (Ordine degli avvocati francofoni e germanofoni) , la vzw Liga voor Mensenrechten , la Ligue des droits humains ASBL , la fondazione privata Ministry of Privacy, la UA, la LV nonché la JU hanno adito la Cour constitutionnelle (Corte costituzionale) con cinque ricorsi diretti all'annullamento parziale o totale della legge del 20 luglio 2022, con la motivazione che quest'ultima violerebbe gli articoli 10, 11, 12, 13, 15, 22, 23 e 29 della Costituzione belga, in combinato disposto con gli articoli 5, 6, 8, 9, 10, 11, 14 e 18 della CEDU , con gli articoli 7, 8, 11, 47 e l'articolo 52, paragrafo 1, della Carta, con l'articolo 5, paragrafo 4, TUE, con l'articolo 6 della direttiva 2002/58, con la direttiva (UE) 2016/680 (9) nonché con il RGPD .

18. Tale giudice considera che solo le censure dei ricorrenti relative agli articoli 5, 6 e 24 della legge del 20 luglio 2022 sollevano dubbi, ai sensi della giurisprudenza derivante dalle sentenze del 6 ottobre 1982, [Cilfit](#) (283/81, EU:C:1982:335) e del 6 ottobre 2021, [Consorzio Italian Management e Catania Multiservizi](#) (C-561/19, EU:C:2021:799), riguardo all'interpretazione dell'articolo 15 della direttiva 2002/58.

19. Anzitutto, per quanto riguarda l'articolo 5 di tale legge, i ricorrenti nel procedimento principale avrebbero in sostanza fatto valere, tra l'altro, che tale articolo impone ai fornitori di servizi di comunicazione elettronica una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione

per periodi lunghi o indeterminati, senza che tale conservazione sia necessaria e limitata allo stretto necessario.

20. Dai lavori preparatori risulterebbe che l'articolo 5, punti 4° e 5°, di detta legge mira a recepire in particolare l'articolo 15, paragrafo 1, della direttiva 2002/58. Il legislatore belga avrebbe precisato, durante tali lavori, che non era possibile prevedere una conservazione di dati «reattiva e mirata fin dall'inizio» a motivo della struttura stessa delle reti e dei servizi interessati. Esso avrebbe inoltre ritenuto che la conservazione dei dati relativi al traffico prevista all'articolo 5, punti 4° e 5°, della medesima legge sia «nell'interesse degli utenti finali dei servizi dell'operatore» e miri a consentire alle vittime di una frode o di un uso illecito della rete di identificare l'autore di questi ultimi. Peraltro, tale conservazione sarebbe presentata, in tali lavori, come «intrinsecamente connessa alla fornitura del servizio di comunicazione elettronica» e tale da consentire la modernizzazione della legge del 13 giugno 2005 alla luce della crescente importanza dell'obiettivo della lotta contro la frode e l'uso illecito della rete nel diritto dell'Unione (Doc. parl., Chambre, 2021-2022, DOC 55 2572/001, pagg. da 26 a 29).

21. Secondo il giudice del rinvio, occorre esaminare se l'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali determinata dall'articolo 122, § 4 e § 4/1, di tale legge, come inserito dall'articolo 5, punti 4° e 5°, della legge del 20 luglio 2022, non produca effetti sproporzionati per le persone i cui dati sono interessati.

22. L'articolo 122, § 4, della legge del 13 giugno 2005 prevedrebbe, a carico degli operatori, un obbligo di conservazione di diversi dati relativi al traffico al fine di «adottare le misure appropriate di cui all'articolo 121/8, § 1, di consentire di accertare la frode o l'uso illecito di rete o del servizio o di identificare il suo autore e la sua origine», a condizione che gli operatori trattino tali dati «nell'ambito della fornitura di tale rete o di tale servizio». I dati relativi al traffico da conservare sarebbero «l'identificativo dell'origine della comunicazione», «l'identificativo della destinazione della comunicazione», «le date nonché le ore precise di inizio e fine della comunicazione» e «l'ubicazione delle apparecchiature terminali delle parti della comunicazione all'inizio e alla fine della comunicazione» (comma 1, punto 1° di tale § 4). Sarebbe inoltre previsto che gli operatori conservino diversi dati relativi al traffico connesso alle comunicazioni in entrata al fine di identificare l'autore della comunicazione, vale a dire «il numero di telefono all'origine della comunicazione in entrata», «l'indirizzo IP utilizzato per l'invio della comunicazione in entrata, la marcatura temporale e la porta utilizzata», nonché «le date e le ore precise di inizio e fine della comunicazione in entrata» (comma 1, punto 2° di detto § 4).

23. Tuttavia, l'elenco dei dati indicati all'articolo 122, § 4, comma 1, di tale legge non sarebbe tassativo, in quanto il comma 2 della medesima disposizione consentirebbe agli operatori di conservare e trattare dati diversi da quelli di cui al comma 1 di tale disposizione, considerati necessari per accertare la frode o l'uso illecito della rete o del servizio o per identificarne l'autore e l'origine. Tale facoltà degli operatori di conservare e di trattare dati diversi da quelli di cui all'articolo 122 § 4, comma 1, di detta legge non

sarebbe soggetta a un parere preventivo dell'Istituto o dell'Autorité de protection des données (Autorità per la protezione dei dati) né a una notifica a tali autorità. I lavori preparatori relativi alla medesima disposizione non fornirebbero alcuna giustificazione in merito a detta facoltà.

24. Inoltre, l'articolo 122 § 4, comma 3, della medesima legge prevedrebbe che: «la Corona può precisare ed estendere, con decreto deliberato in Consiglio dei ministri, e previo parere dell'[Istituto] e dell'Autorité de protection des données (Autorità per la protezione dei dati), i dati relativi al traffico la cui conservazione deve essere considerata necessaria per il perseguimento degli obiettivi previsti al presente paragrafo». I lavori preparatori giustificerebbero detta facoltà con il fatto che le frodi evolvono in modo significativo nel tempo e che i dati conservati possono differenziarsi a seconda del tipo di servizio di comunicazione elettronica, delle dimensioni dell'operatore, degli strumenti di cui quest'ultimo dispone e degli utenti di tale servizio.

25. Per quanto riguarda i termini di conservazione, i dati di cui all'articolo 122, § 4, comma 1, punto 1°, della legge del 13 giugno 2005 sarebbero, in linea di principio, conservati per quattro mesi, mentre i dati di cui all'articolo 122, § 4, comma 1, punto 2°, di tale legge, lo sarebbero per dodici mesi. Tali termini di conservazione potrebbero essere prorogati. A tal riguardo, l'articolo 122, § 4, comma 1, punto 3°, di detta legge disporrebbe che i dati di cui al punto 1°, relativi a una frode specifica o a un uso illecito specifico della rete, possono essere conservati «per il tempo necessario alla sua analisi e alla sua soluzione, eventualmente oltre il termine di quattro mesi di cui al punto 1°». Inoltre, l'articolo 122, § 4, punto 4°, di tale medesima legge, preciserebbe che i dati di cui al punto 2° di tale disposizione, relativi a un uso illecito specifico della rete, possono essere conservati «per il tempo necessario al trattamento dello stesso, se del caso oltre il termine di dodici mesi menzionato al punto 2°».

26. L'articolo 122, § 4/1, della legge del 13 giugno 2005 prevede a sua volta, a carico degli operatori, la possibilità di conservare e di trattare i dati «necessari per garantire la sicurezza e il buon funzionamento delle loro reti e dei loro servizi di comunicazione elettronica, e in particolare per accertare e analizzare un attentato potenziale o reale per tale sicurezza, ivi compreso per individuare l'origine di detto attentato». Neanche tale facoltà degli operatori sarebbe soggetta a un parere preventivo dell'Istituto o dell'Autorité de protection des données (Autorità per la protezione dei dati) né a una notifica a tali autorità. I dati così considerati, in forza dell'articolo 122, § 4/1, comma 3, di tale legge, in linea di principio, potrebbero essere conservati per un periodo di dodici mesi. I dati relativi a un attentato «specifico» alla sicurezza della rete potrebbero essere tuttavia conservati «per l'arco di tempo necessario per trattarlo, se del caso oltre il termine di dodici mesi di cui al comma 2».

27. Il giudice del rinvio conclude che l'articolo 122, § 4, di detta legge prevede una conservazione generalizzata e sistematica dei dati relativi al traffico cui si riferisce e che l'obbligo di conservazione dei dati non costituisce l'eccezione, bensì la regola. Tale constatazione sarebbe tanto più valida in quanto, ai sensi dell'articolo 122, § 4, comma 4,

della medesima legge, i dati relativi al traffico conservati dagli operatori che presentano un nesso con una frode presunta o con un uso illecito presunto possono essere trasferiti alle autorità competenti, in particolare alle autorità giudiziarie, ai servizi di polizia e agli ufficiali di polizia giudiziaria dell'Istituto, cosicché la conservazione e il trattamento di dati effettuati dagli operatori sulla base dell'articolo 122, § 4, della legge del 13 giugno 2005 possono dar luogo ad azioni penali.

28. Per quanto riguarda l'articolo 122, § 4/1, di tale legge, il giudice del rinvio osserva che tale disposizione non precisa quali dati possano essere conservati. Peraltro, i dati relativi a un «attentato specifico» alla sicurezza della rete potrebbero essere conservati «oltre il termine di dodici mesi di cui al comma 2», senza che sia precisato, nel testo dell'articolo 122, § 4/1, di detta legge né nei lavori preparatori della legge del 20 luglio 2022, in che cosa consista un «attentato specifico».

29. Orbene, il giudice del rinvio osserva che la Corte non si è ancora pronunciata sull'interpretazione dell'articolo 15 della direttiva 2002/58 quando sono in discussione misure di conservazione dei dati relativi alle comunicazioni elettroniche al fine di garantire la prevenzione, la ricerca, l'accertamento e il perseguimento dell'uso non autorizzato del sistema di comunicazione elettronica. Inoltre, i punti di vista delle parti sull'interpretazione dell'articolo 15, paragrafo 1, di tale direttiva, dinanzi ad essa esposti, divergerebbero.

30. Quanto poi all'articolo 6 della legge del 20 luglio 2022, il giudice del rinvio rileva che le censure dei ricorrenti riguarderebbero la conservazione dei dati relativi all'ubicazione, diversi dai dati relativi al traffico, che rientrano nell'ambito di applicazione dell'articolo 15, paragrafo 1, di detta direttiva e che sono previsti dall'articolo 123, § 1, punti 1º, 2º e 5º, della legge del 13 giugno 2005, come sostituito dall'articolo 6 della legge del 20 luglio 2022.

31. L'articolo 123, § 1, della legge del 13 giugno 2005 prevedrebbe che gli operatori interessati possano conservare e trattare i dati relativi all'ubicazione, relativi a un abbonato o a un utente finale, solo «qualora ciò sia necessario per il buon funzionamento e la sicurezza della rete o del servizio» (punto 1º di tale § 1º) e «qualora ciò sia necessario per accertare o analizzare le frodi o un uso illecito della rete» (punto 2º di detto § 1º). I dati di cui all'articolo 123, § 1, punto 1º, di tale legge sarebbero, in linea di principio, conservati per dodici mesi a decorrere dalla data della comunicazione e quelli di cui all'articolo 123, § 1, punto 2º, di detta legge sarebbero conservati, in linea di principio, per quattro mesi.

32. Le ipotesi di cui all'articolo 123, § 1, punti 1º e 2º, della medesima legge tenterebbero di garantire la prevenzione, la ricerca, l'accertamento e il perseguimento dell'uso non autorizzato del sistema di comunicazione elettronica ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58.

33. Spetterebbe al giudice del rinvio verificare se l'ingerenza determinata da tali disposizioni nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali sia necessaria, ragionevole e proporzionata all'interno di una società democratica al fine di prevenire l'uso non autorizzato del sistema di comunicazione elettronica. A tal riguardo, il giudice del rinvio rileva che spetta agli operatori individuare i dati relativi all'ubicazione diversi dai dati relativi al traffico che ritengono necessario conservare e trattare. Tali operatori valuterebbero altresì, in ciascun caso, la necessità di tale conservazione e di tale trattamento. Peraltro, sarebbe previsto che la durata di dodici mesi possa essere prorogata «in caso di attentato specifico alla sicurezza della rete che richieda di prolungare la conservazione dei dati di cui trattasi oltre tale termine» e che il suddetto periodo di quattro mesi possa essere prorogato «in caso di frode specifica o di uso illecito specifico che richieda di prolungare la conservazione dei dati di cui trattasi oltre tale termine». Infine, spetterebbe ai detti operatori decidere se occorra prorogare il periodo di conservazione.

34. Per le stesse ragioni che potrebbero essere invocate per quanto riguarda l'articolo 5 della legge del 20 luglio 2022, l'articolo 6 di tale legge solleverebbe un dubbio quanto all'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58.

35. Per quanto riguarda, infine, l'articolo 24 di detta legge, il giudice del rinvio rileva che tale disposizione inserisce, nella legge del 17 gennaio 2003, un articolo 25/1 che disciplina l'accesso dell'ufficiale di polizia giudiziaria dell'Istituto ai metadati. Le censure del ricorrente che chiedono l'annullamento di tale articolo 24 riguarderebbero la violazione dei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, garantiti dall'articolo 22 della Costituzione belga, dall'articolo 8 della CEDU, dagli articoli 7, 8 e dall'articolo 52, paragrafo 1, della Carta, dalla direttiva 2002/58, dalla direttiva 2016/680 e dal RGPD. Dato che l'articolo 24 della legge del 20 luglio 2022 rinvia agli articoli 5 e 6 della medesima legge in merito ai quali occorrerebbe sottoporre questioni pregiudiziali alla Corte, il giudice del rinvio considera che occorre sospendere il procedimento sull'esame delle censure relative a tale articolo 24, in attesa della risposta della Corte a tali questioni pregiudiziali.

36. È in tale contesto che la Cour constitutionnelle (Corte costituzionale) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se l'articolo 15, paragrafo 1, della [direttiva 2002/58], in combinato disposto con gli articoli 7 [ e 8 nonché l'articolo] 52, paragrafo 1, della [Carta], debba essere interpretato nel senso che:

a) esso osta a una normativa nazionale che prevede un obbligo per gli operatori di servizi di comunicazione elettronica di conservare e trattare i dati relativi al traffico oggetto di tale normativa nell'ambito della fornitura della rete o del servizio di cui trattasi, per un periodo di quattro o dodici mesi, a seconda dei casi, affinché essi adottino le misure appropriate, proporzionate, preventive e riparatorie per impedire le frodi e gli usi illeciti delle loro reti ed

evitare di arrecare danni agli utenti finali o di infastidirli, e per accertare o analizzare le frodi o gli usi illeciti della rete o del servizio o poterne identificare gli autori e l'origine;

b) esso osta a una normativa nazionale che consente a detti operatori di conservare e trattare i dati relativi al traffico oltre i termini suindicati, in caso di frode specifica accertata o di uso illecito specifico della rete accertato, per il tempo necessario alla sua analisi e alla sua soluzione o per il tempo necessario al trattamento di tale uso illecito;

c) esso osta a una normativa nazionale che, senza prevedere l'obbligo di richiesta di un parere preventivo o di notifica a un'autorità indipendente, consente a detti operatori di conservare e trattare altri dati, diversi da quelli menzionati dalla legge, al fine di accertare la frode o l'uso illecito della rete o del servizio, o di identificarne l'autore e l'origine;

d) esso osta a una normativa nazionale che, senza prevedere l'obbligo di richiesta di un parere preventivo o di notifica a un'autorità indipendente, consente a detti operatori di conservare e trattare per un periodo di dodici mesi i dati relativi al traffico che ritengano necessari per garantire la sicurezza e il buon funzionamento delle loro reti e dei loro servizi di comunicazione elettronica, e in particolare per accertare e analizzare un attentato potenziale o reale a tale sicurezza, compreso l'accertamento dell'origine di tale attentato e, in caso di attentato specifico alla sicurezza della rete, per l'arco di tempo necessario al suo trattamento.

2) Se l'articolo 15, paragrafo 1, della [direttiva 2002/58], in combinato disposto con gli articoli 7[ e 8 nonché l'articolo]52, paragrafo 1, della [Carta], debba essere interpretato nel senso che:

a) esso osta a una normativa nazionale che consente agli operatori di reti mobili di conservare e trattare i dati relativi all'ubicazione, senza che la normativa descriva con precisione quali dati siano interessati, nell'ambito della fornitura della rete o del servizio in oggetto, per un periodo di quattro o dodici mesi, a seconda dei casi, quando sia necessario per il buon funzionamento e la sicurezza della rete o del servizio, o per accertare o analizzare le frodi o l'uso illecito della rete;

b) esso osta a una normativa nazionale che consente a tali operatori di conservare e trattare i dati relativi all'ubicazione oltre i termini suindicati, in caso di attentato specifico, di frode specifica o di uso illecito specifico.

3) Qualora, sulla base delle risposte fornite alla prima o alla seconda questione pregiudiziale, la Cour constitutionnelle (Corte costituzionale) giunga alla conclusione che determinate disposizioni della [legge del 20 luglio 2022] violano uno o più obblighi derivanti dalle disposizioni che tali questioni menzionano, se possano essere mantenuti provvisoriamente gli effetti delle succitate disposizioni della legge del 20 luglio 2022, al fine di evitare una situazione di incertezza del diritto e di permettere che i dati raccolti e conservati in precedenza possano ancora essere utilizzati per il raggiungimento degli obiettivi previsti dalla legge».

37. Hanno presentato osservazioni scritte la Ligue des droits humains, i governi belga, estone, irlandese, spagnolo e finlandese nonché la Commissione europea. Le medesime parti, nonché l'Académie Fiscale e il governo italiano hanno presentato osservazioni orali all'udienza che si è tenuta 14 aprile 2026.

#### IV. **Analisi**

##### A. **Osservazioni preliminari**

38. La questione della compatibilità dei regimi nazionali di conservazione e di accesso ai dati relativi al traffico e all'ubicazione con l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7 e 8 della Carta, è stata esaminata in numerose occasioni dalla Corte.

39. Tuttavia, la Corte continua ad essere regolarmente interpellata al riguardo. La persistenza dei rinvii pregiudiziali relativi all'interpretazione di tali disposizioni si spiega certamente con il carattere eminentemente casistico delle questioni sottoposte alla Corte in tale materia. Non si può quindi ignorare che tale giurisprudenza è stata recentemente oggetto di sviluppi sostanziali, in quanto la Corte è stata investita per la prima volta della questione della conservazione e dell'accesso a dati relativi al traffico ai fini dell'accertamento e del perseguimento di reati commessi esclusivamente online. Appare quindi opportuno procedere ad un breve richiamo della giurisprudenza, in particolare dei suoi sviluppi più recenti (sezione B).

40. Tuttavia, tale persistenza può anche essere indice delle difficoltà che i giudici nazionali possono incontrare nella loro prassi quotidiana nell'attuare la giurisprudenza della Corte quando sono chiamati a valutare la compatibilità con il diritto dell'Unione di disposizioni nazionali relative alla conservazione e all'accesso ai dati relativi al traffico e all'ubicazione. Infatti, mi sembra che la giurisprudenza pertinente della Corte possa apparire, a causa del suo sviluppo casistico, complessa, se non addirittura, per taluni aspetti, di difficile lettura (sezione C).

41. Cercherò pertanto di procedere a una sistematizzazione della giurisprudenza della Corte relativa alla conservazione dei dati relativi al traffico e all'ubicazione (sezione D), prima di esaminare, alla luce di tali principi, le questioni pregiudiziali sottoposte alla Corte nella presente causa (sezione E).

##### B. **Giurisprudenza relativa all'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58 per quanto riguarda regimi volti alla conservazione dei dati relativi al traffico e all'ubicazione**

###### 1. ***Eccezione prevista all'articolo 15, paragrafo 1, della direttiva 2002/58***

42. La direttiva 2002/58 enuncia una serie di principi relativi alla conservazione e al trattamento da parte dei fornitori di servizi di comunicazione elettronica dei dati relativi al traffico e all'ubicazione.

43. Anzitutto, l'articolo 5, paragrafo 1, di tale direttiva sancisce il principio di riservatezza sia delle comunicazioni elettroniche sia dei dati relativi al traffico a queste correlati e implica, in particolare, il divieto imposto, in linea di principio, a qualsiasi persona diversa dagli utenti di memorizzare, senza il loro consenso, tali comunicazioni e dati ([10](#)).

44. Inoltre, l'articolo 6, paragrafo 1, di detta direttiva prevede che i dati sul traffico relativi agli abbonati e agli utenti devono essere cancellati e resi anonimi quando non sono più necessari per la trasmissione di una comunicazione ([11](#)).

45. L'articolo 9 della medesima direttiva prevede, infine, che i dati relativi all'ubicazione diversi dai dati relativi al traffico, possono essere trattati soltanto in presenza di determinate condizioni e dopo essere stati resi anonimi o con il consenso degli utenti o degli abbonati ([12](#)).

46. Così, adottando la direttiva 2002/58, il legislatore dell'Unione ha concretizzato i diritti sanciti dagli articoli 7 e 8 della Carta, di modo 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, in mancanza del loro consenso, rimangano anonimi e non possano essere registrati. Pertanto, tale direttiva non si limita a disciplinare l'accesso a tali dati mediante garanzie dirette a prevenire gli abusi, ma sancisce altresì, in particolare, il principio del divieto della loro memorizzazione da parte di terzi ([13](#)).

47. L'articolo 15, paragrafo 1, di detta direttiva consente specificamente agli Stati membri di adottare misure legislative volte a «limitare» i diritti e gli obblighi previsti, segnatamente, agli articoli 5, 6 e 9 di tale direttiva, come quelli derivanti dai principi di riservatezza delle comunicazioni e del divieto di memorizzazione dei dati ad esse correlati.

48. Tale disposizione stabilisce peraltro un elenco degli obiettivi idonei a giustificare una limitazione dei diritti e degli obblighi previsti, in particolare, agli articoli 5, 6 e 9 della direttiva 2002/58. Può quindi trattarsi di salvaguardare la sicurezza nazionale, la difesa e la sicurezza pubblica, oppure di garantire la prevenzione, la ricerca, l'accertamento e il perseguimento di reati o l'uso non autorizzato del sistema di comunicazione elettronica. La Corte ha già dichiarato che l'elenco degli obiettivi di cui all'articolo 15, paragrafo 1, prima frase, di tale direttiva ha carattere tassativo, di modo che una misura legislativa adottata ai sensi di detta disposizione deve rispondere in modo effettivo e rigoroso ad uno di questi obiettivi ([14](#)).

49. L'articolo 15, paragrafo 1, di detta direttiva costituisce quindi un'eccezione alla regola generale dettata da tali disposizioni e deve pertanto, conformemente a una giurisprudenza costante, essere oggetto di un'interpretazione restrittiva ([15](#)).

50. Così facendo, l'articolo 15, paragrafo 1, della medesima direttiva, riflette altresì la circostanza che i diritti sanciti dagli articoli 7, 8 e 11 della Carta non appaiono come

prerogative assolute, ma vanno considerati alla luce della loro funzione sociale. Infatti, come risulta dal suo articolo 52, paragrafo 1, la Carta ammette limitazioni all'esercizio di tali diritti, purché tali limitazioni siano previste dalla legge, rispettino il contenuto essenziale dei summenzionati diritti e, nel rispetto del principio di proporzionalità, siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. Pertanto, l'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce della Carta, richiede che si tenga conto allo stesso modo dell'importanza degli obiettivi di salvaguardia della sicurezza nazionale e di lotta alle forme gravi di criminalità nel contribuire alla protezione dei diritti e delle libertà altrui e di quella dei diritti sanciti agli articoli 3, 4, 6 e 7 della Carta, dai quali possono derivare obblighi positivi a carico dei pubblici poteri (16).

51. La Corte dichiara quindi in modo costante che a fronte di questi diversi obblighi positivi, occorre procedere al contemperamento dei diversi interessi legittimi e dei diritti in gioco. In tale contesto, dalla formulazione stessa dell'articolo 15, paragrafo 1, prima frase, di tale direttiva discende che gli Stati membri possono adottare una misura che deroghi al principio di riservatezza qualora tale misura sia «necessaria, opportuna e proporzionata all'interno di una società democratica». Il considerando 11 di detta direttiva precisa al riguardo che una misura siffatta deve essere «strettamente» proporzionata allo scopo perseguito (17).

## **2. *Proporzionalità quale elemento centrale dell'analisi di un regime di conservazione dei dati, alla luce dell'articolo 15, paragrafo 1, della direttiva 2002/58***

52. Come avevo affermato nelle mie seconde conclusioni nella causa *Quadrature du Net e a. (Dati personali e lotta alla contraffazione)*, il principio di proporzionalità è quindi al centro dell'analisi di una misura nazionale di conservazione dei dati relativi al traffico e all'ubicazione alla luce dell'articolo 15, paragrafo 1, della direttiva 2002/58, e si articola in due parti (18).

53. Da un lato, la Corte dichiara che per soddisfare il requisito di proporzionalità, una normativa deve prevedere norme chiare e precise che disciplinino la portata e l'applicazione della misura considerata e impongano requisiti minimi in modo che le persone i cui dati personali sono oggetto di attenzione dispongano di garanzie sufficienti che consentano di proteggere efficacemente tali dati contro i rischi di abuso. Tale normativa deve essere giuridicamente vincolante nell'ambito dell'ordinamento nazionale e, in particolare, indicare in quali circostanze e a quali condizioni una misura che preveda il trattamento di siffatti dati possa essere adottata, garantendo così che l'ingerenza sia limitata allo stretto necessario (19). In altri termini, occorre garantire che il regime di cui trattasi risponda a una serie di condizioni volte a limitare la portata dell'ingerenza che esso presuppone.

54. D'altro lato, secondo una giurisprudenza costante, la possibilità per gli Stati membri di giustificare una limitazione dei diritti e degli obblighi previsti, segnatamente,

agli articoli 5, 6 e 9 della direttiva 2002/58 deve essere valutata misurando la gravità dell'ingerenza che una restrizione siffatta comporta e verificando che l'importanza dell'obiettivo di interesse generale perseguito da tale limitazione sia adeguata a tale gravità (20). In altri termini, si tratta di garantire che l'importanza degli obiettivi perseguiti corrisponda al livello di gravità dell'ingerenza che il regime di conservazione dei dati relativi al traffico e all'ubicazione comporta. Infatti, secondo la Corte, esiste una gerarchia tra tali obiettivi in funzione della loro rispettiva importanza (21), in quanto la salvaguardia della sicurezza nazionale può giustificare ingerenze più rilevanti nei diritti fondamentali, laddove la lotta contro la criminalità in generale può fondare solo ingerenze di minore gravità.

55. È sulla base di tali principi che la Corte ha dichiarato, in particolare, che una misura nazionale che prevede la conservazione generalizzata e indifferenziata dei dati relativi al traffico e all'ubicazione può essere giustificata soltanto dall'obiettivo di salvaguardia della sicurezza nazionale (22), mentre è escluso che una siffatta misura possa essere giustificata dall'obiettivo di lotta contro la criminalità in generale (23).

56. Nello stesso ordine di idee, la Corte ammette la possibilità di una conservazione *mirata* degli stessi dati, in particolare sulla base di un criterio geografico, al fine di perseguire l'obiettivo della lotta contro la criminalità *grave* (24), e della conservazione degli indirizzi IP attribuiti all'origine di una connessione allo scopo di perseguire questo stesso obiettivo (25).

57. Per contro, per quanto riguarda i dati relativi all'identità civile degli utenti, essi possono, a causa del minor grado di ingerenza nei diritti fondamentali che la loro conservazione presuppone, esserne oggetto allo scopo di lottare contro la criminalità in generale (26).

58. Tale approccio è anche quello seguito dalla Corte EDU. In sede di esame di un'eventuale violazione dell'articolo 8 della CEDU da parte di una misura nazionale che prevede la conservazione di taluni dati relativi al traffico e all'ubicazione, la Corte EDU fa della proporzionalità di tale misura l'elemento centrale della sua analisi. Pertanto, in considerazione della gravità dell'ingerenza considerata nell'esercizio da parte dei ricorrenti dei loro diritti rientranti nella sfera dell'articolo 8 della CEDU (27), essa dichiara che una normativa nazionale che prevede la conservazione generalizzata e indifferenziata di dati di comunicazione viola tale articolo in quanto è insufficiente a limitare a quanto necessario in una società democratica l'ingerenza che essa comporta nel diritto al rispetto della vita privata (28).

### **3. Recente adeguamento della giurisprudenza relativa all'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58 per quanto riguarda atti di criminalità commessi esclusivamente online**

59. Più di recente, la Corte ha precisato l'esame della proporzionalità di una misura di conservazione di taluni dati relativi al traffico e all'ubicazione, quando tale misura mira

all'accertamento e al perseguimento di reati commessi esclusivamente online (29). La Corte ha quindi modulato la sua interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58 sotto due profili.

60. In primo luogo, la Corte ha affinato l'esame della gravità dell'ingerenza determinata da una misura di conservazione di taluni dati relativi al traffico e all'ubicazione – nel caso di specie, di indirizzi IP attribuiti all'origine di una connessione. Pertanto, la Corte dichiara che una misura, ai sensi dell'articolo 15, paragrafo 1, di tale direttiva, che consente la conservazione generalizzata e indifferenziata di tali indirizzi IP può, se del caso, essere giustificata dall'obiettivo della lotta contro i reati in generale (30), qualora sia effettivamente escluso che tale conservazione possa generare ingerenze gravi nella vita privata dell'interessato per effetto della possibilità di trarre conclusioni precise su quest'ultimo mediante, in particolare, un collegamento di tali indirizzi IP con un insieme di dati relativi al traffico o all'ubicazione che siano stati parimenti conservati da tali fornitori (31).

61. La Corte precisa peraltro che uno Stato membro che intenda imporre ai fornitori di servizi di comunicazione elettronica un siffatto obbligo deve assicurarsi che le modalità di conservazione di detti dati siano tali da garantire che sia esclusa qualsiasi combinazione di detti indirizzi IP con altri dati conservati che consentano di trarre conclusioni precise sulla vita privata delle persone i cui dati siano conservati (32). Spetta quindi ad esso prevedere modalità di conservazione di tali dati che devono riguardare la struttura stessa di detta conservazione che, in sostanza, deve essere organizzata in modo da garantire una separazione effettivamente stagna delle diverse categorie di dati conservati (33).

62. La sentenza *Quadrature du Net II* costituisce quindi un'evoluzione della giurisprudenza precedente relativa all'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58. Non solo è chiaramente enunciato che la gravità dell'ingerenza dipende dalle conclusioni che è possibile trarre sulla vita privata delle persone i cui dati sono conservati, ma la Corte ammette, inoltre, che gli Stati membri hanno la possibilità, prevedendo modalità specifiche di conservazione dei dati di cui trattasi, di influire sul livello di gravità di un'ingerenza (34).

63. In secondo luogo, la Corte ricorda che, nel caso di reati commessi online, l'accesso a taluni dati, in particolare l'indirizzo IP all'origine di una connessione, può costituire l'unico strumento di indagine che consente l'identificazione effettiva della persona alla quale tale indirizzo era attribuito al momento della commissione del reato in questione (35).

64. Secondo la Corte, questa sola circostanza tende a dimostrare che la conservazione dei dati pertinenti è, per quanto riguarda la lotta contro i reati commessi online, strettamente necessaria al conseguimento dell'obiettivo perseguito e soddisfa quindi il requisito di proporzionalità imposto dall'articolo 15, paragrafo 1, della direttiva 2002/58 (36). Infatti, la mancanza di conservazione di tali dati (e di successivo accesso ai medesimi) comporta un rischio di impunità sistemica dei reati commessi online che non

può essere ignorato al fine di valutare, nell'ambito di un bilanciamento dei diversi diritti e interessi in gioco, se un'ingerenza nei diritti garantiti dagli articoli 7, 8 e 11 della Carta sia una misura proporzionata alla luce dell'obiettivo della lotta contro i reati (37).

65. Così facendo, mi sembra che la sentenza *Quadrature du Net II* conduca a un certo allentamento della giurisprudenza della Corte relativa all'articolo 15, paragrafo 1, di tale direttiva o, quantomeno, a un'applicazione pragmatica dei suoi principi.

66. La sua lettura complessiva rivela tuttavia, a mio avviso, taluni limiti.

**C. Insidie della giurisprudenza relativa all'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58 per quanto riguarda regimi volti alla conservazione dei dati relativi al traffico e all'ubicazione**

67. Mi sembra che la coesistenza di una giurisprudenza flessibile, per quanto riguarda la conservazione di dati necessari alla lotta contro i reati commessi online conformemente all'articolo 15, paragrafo 1, della direttiva 2002/58, e della giurisprudenza classica della Corte relativa all'interpretazione di tale disposizione, produca due limiti.

68. In primo luogo, e da un punto di vista pratico, rilevo che la lettura combinata della sentenza *Quadrature du Net II* e delle sentenze precedenti porta a richiedere ai fornitori di servizi di comunicazione elettronica la proliferazione di file di conservazione dei dati, che devono rispondere a diverse caratteristiche tecniche, a seconda dell'obiettivo perseguito da tale conservazione.

69. Se una siffatta problematica poteva già esistere, prima della sentenza *Quadrature du Net II*, a causa dei diversi regimi di conservazione dei dati a seconda dell'obiettivo perseguito, essa appare ora ancor più pregnante.

70. La giurisprudenza della Corte impone infatti ormai agli Stati membri di prevedere, quando impongono, per il perseguimento di un obiettivo di minore importanza rispetto alla difesa della sicurezza nazionale, la conservazione di dati relativi al traffico e all'ubicazione che consentano, in linea di principio, di trarre conclusioni precise sulla vita privata degli utenti, modalità di conservazione che garantiscano che le diverse categorie di dati siano conservate in modo completamente separato (38).

71. Secondo la giurisprudenza della Corte, tali modalità di conservazione devono garantire che, sul piano tecnico, la separazione delle diverse categorie di dati conservati sia effettivamente stagna, mediante un *dispositivo informatico sicuro e affidabile* (39). Inoltre, la messa in relazione dei diversi dati così conservati deve avvenire mediante l'uso di un procedimento tecnico efficiente che non metta a rischio l'efficacia della separazione stagna di tali categorie di dati (40). Peraltro, l'affidabilità di tale separazione stagna deve essere oggetto di un controllo regolare da parte di un'autorità pubblica diversa da quella che cerca di ottenere l'accesso ai dati personali conservati dai fornitori di servizi di comunicazione elettronica (41).

72. Pertanto, la conservazione dei dati relativi al traffico e all'ubicazione necessari all'accertamento e al perseguimento dei reati commessi esclusivamente online presuppone, per essere effettuata conformemente all'articolo 15, paragrafo 1, della direttiva 2002/58, una serie di adeguamenti tecnici da parte dei fornitori di servizi di comunicazione elettronica.

73. Orbene, non esiste alcun requisito del genere per quanto riguarda i dati relativi al traffico e all'ubicazione conservati allo scopo di far fronte a una minaccia grave per la sicurezza nazionale. In una siffatta ipotesi tali dati possono essere conservati in un unico archivio, agevolando così le sovrapposizioni tra gli stessi, senza che ciò rimetta in discussione la compatibilità di un siffatto meccanismo con l'articolo 15, paragrafo 1, di tale direttiva.

74. Ne consegue che i requisiti derivanti dalla giurisprudenza della Corte relativa all'interpretazione di tale disposizione mi sembrano condurre alla proliferazione dei file di conservazione di dati relativi al traffico e all'ubicazione, che rispondono inoltre a caratteristiche diverse.

75. Una siffatta soluzione comporta, a mio avviso, un rischio non trascurabile quanto alla sicurezza dei dati relativi al traffico e all'ubicazione che devono essere conservati in un archivio che ne garantisca la separazione stagna, in modo che non si possano trarre conclusioni precise sulla vita degli utenti. Poiché gli stessi dati sono oggetto di due diverse modalità di conservazione, non si può escludere il ricorso, quanto meno accidentale, al file meno sicuro per ottenere dati al di fuori di una grave minaccia per la sicurezza nazionale.

76. Inoltre, come sottolineato dalla Ligue des droits humains in udienza, mi sembra che la proliferazione di file di conservazione per dati identici comporti anche il rischio di mancata attuazione effettiva della giurisprudenza più recente della Corte. Poiché tutti i dati relativi al traffico e all'ubicazione sono già raccolti in un unico archivio a fini di salvaguardia della sicurezza nazionale, esiste una probabilità non trascurabile che i fornitori di servizi di comunicazione elettronica non procedano, in definitiva, ad alcuna strutturazione dei dati quando questi ultimi sono conservati per il perseguimento di altri obiettivi enunciati all'articolo 15, paragrafo 1, della direttiva 2002/58.

77. In secondo luogo, una lettura complessiva della giurisprudenza della Corte relativa all'interpretazione dell'articolo 15, paragrafo 1, di tale direttiva mi induce a pormi interrogativi sulla logica stessa di quest'ultima.

78. Infatti, risulta chiaramente dalla stessa che la gravità dell'ingerenza determinata dalla conservazione dei dati relativi al traffico e all'ubicazione attiene alle conclusioni che è possibile trarre da tali dati per quanto riguarda la vita privata degli utenti. Inoltre, la Corte ammette che l'ingerenza possa essere limitata da misure tecniche volte proprio a garantire che tali conclusioni non possano essere tratte.

79. Da tali elementi, al centro del test di proporzionalità di cui all'articolo 15, paragrafo 1, della direttiva 2002/58, risulta, a mio avviso, che la determinazione del livello di ingerenza nei diritti fondamentali dipende essenzialmente dal successivo utilizzo che può essere fatto dei dati di cui trattasi.

80. È vero che la Corte dichiara in modo costante che la conservazione dei dati relativi al traffico e all'ubicazione costituisce un'ingerenza nei diritti fondamentali a prescindere dalla circostanza che le informazioni relative alla vita privata di cui trattasi abbiano o meno un carattere sensibile o che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a siffatta ingerenza (42). Parimenti, è irrilevante la circostanza che i dati conservati siano o meno utilizzati successivamente, in quanto l'accesso a tali dati costituisce, a prescindere dall'uso che ne viene fatto in seguito, un'ingerenza distinta nei diritti fondamentali (43).

81. Non si tratta quindi, in questo caso, di contestare l'idea che la sola conservazione dei dati relativi al traffico e all'ubicazione sia, di per sé, un'ingerenza nei diritti fondamentali.

82. Tuttavia, mi sembra che tale ingerenza derivi anzitutto dal fatto che tali dati possono essere utilizzati in modo da trarre conclusioni sulla vita privata degli utenti. La Corte sottolinea del resto quanto segue: la conservazione di dati viene effettuata al solo scopo di rendere, eventualmente, tali dati accessibili alle autorità nazionali competenti (44). Infatti, in mancanza di conservazione dei dati relativi al traffico e all'ubicazione, la questione dell'ingerenza determinata dall'accesso a questi ultimi non si pone (45).

83. In altri termini, a mio avviso, la conservazione dei dati relativi al traffico e all'ubicazione costituisce un'ingerenza nei diritti fondamentali, in quanto costituisce la condizione necessaria per il loro successivo accesso, indipendentemente dal fatto che tale accesso avvenga o meno.

84. Così facendo, ritengo, al pari della Commissione, che un regime di conservazione generalizzata e indifferenziata dei dati relativi al traffico e all'ubicazione non debba essere escluso a priori dal momento che esso non riguarda la salvaguardia della sicurezza nazionale. Infatti, nella misura in cui un tale regime rimane soggetto a modalità di strutturazione nella conservazione di tali dati come quelle elaborate dalla Corte nella sentenza *Quadrature du Net II* e a limiti temporali rigorosi, mi sembra che l'ingerenza nei diritti fondamentali che esso implica resti proporzionata.

85. Ciò vale a maggior ragione in quanto la giurisprudenza della Corte, anche precedente alla sentenza *Quadrature du Net II*, mi sembra recare in sé le premesse di una siffatta soluzione. Infatti, ammettendo la possibilità della conservazione dei dati sulla base di un criterio geografico, per motivi diversi da quelli relativi alla salvaguardia della sicurezza nazionale (46), la Corte riconosce implicitamente che una conservazione

generalizzata e indifferenziata di tali dati può, a determinate condizioni, essere ammessa ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58.

86. Per contro, il fatto di ammettere la compatibilità di un siffatto regime di conservazione dei dati relativi al traffico e all'ubicazione con l'articolo 15, paragrafo 1, di tale direttiva non può che andare di pari passo con un rafforzamento significativo delle condizioni relative all'accesso a tali dati, in particolare quando tale accesso è richiesto allo scopo di perseguire gli obiettivi di minore importanza nella gerarchia di tale disposizione.

87. In particolare, e in modo schematico, l'accesso ai dati così conservati dovrebbe essere negato qualora sia giustificato da un obiettivo dell'articolo 15, paragrafo 1, di detta direttiva di minore importanza, sebbene l'ingerenza nei diritti fondamentali che esso comporta presenti un grado di gravità rilevante. In altri termini, il requisito della corrispondenza tra la gravità dell'ingerenza nei diritti fondamentali e l'importanza dell'obiettivo perseguito non viene meno, ma si concentra nella fase dello studio dell'ingerenza nei diritti fondamentali derivante di detto accesso.

88. Una siffatta soluzione consentirebbe anzitutto, a mio avviso, di ovviare al rischio di impunità sistemica dei reati commessi esclusivamente online o la cui commissione o preparazione è agevolata dalle caratteristiche proprie di Internet. Essa garantisce infatti l'esistenza dei dati necessari al loro perseguimento, mentre lo sviluppo e l'importanza sempre crescente di Internet comportano nel contempo l'aumento dei comportamenti di criminalità informatica (47).

89. Inoltre, accompagnata da un rafforzamento delle condizioni che consentono l'accesso ai dati pertinenti, tale soluzione garantisce nel contempo la limitazione dell'ingerenza nei diritti fondamentali determinata da una siffatta conservazione.

90. Infine, evitando la proliferazione delle tecniche di conservazione di tali dati, detta soluzione consente altresì di evitare l'elusione, negli Stati membri, della giurisprudenza della Corte – accidentale o meno – tramite l'accesso, per motivi estranei alla difesa della sicurezza nazionale, ai dati conservati in un archivio generale non strutturato allo scopo di perseguire quest'ultimo obiettivo, o tramite la sua mancata effettiva attuazione da parte dei fornitori di servizi di comunicazione elettronica.

91. Pertanto, ritengo che sia possibile, e persino auspicabile, estendere la soluzione elaborata dalla Corte nella sentenza *Quadrature du Net II* a tutti i regimi di conservazione dei dati relativi al traffico e all'ubicazione adottati sulla base dell'articolo 15, paragrafo 1, della direttiva 2002/58 (48).

#### D. **Proposta di sistematizzazione**

92. L'articolo 15, paragrafo 1, della direttiva 2002/58 dovrebbe essere quindi interpretato nel senso che esso non osta a una normativa nazionale che prevede, per il perseguimento degli obiettivi enunciati in tale disposizione, la conservazione generalizzata e indifferenziata dei dati relativi al traffico e all'ubicazione, a condizione

che, in forza di tale normativa, tali dati siano conservati in condizioni e secondo modalità tecniche che garantiscano che sia escluso che tale conservazione possa consentire di trarre conclusioni precise sulla vita privata degli utenti, il che può essere conseguito, in particolare, imponendo ai fornitori di servizi di comunicazione elettronica un obbligo di conservazione delle diverse categorie di dati personali che garantisca una separazione effettivamente stagna di tali diverse categorie di dati impedendo, nella fase di tale conservazione, qualsiasi utilizzo combinato di tali diverse categorie di dati e per un periodo di tempo non superiore allo stretto necessario.

93. Una siffatta normativa deve inoltre prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura considerata e impongano requisiti minimi in modo che le persone i cui dati personali sono oggetto di attenzione dispongano di garanzie sufficienti che consentano di proteggere efficacemente tali dati contro i rischi di abuso. Detta normativa deve essere giuridicamente vincolante nell'ambito dell'ordinamento nazionale e, in particolare, indicare in quali circostanze e a quali condizioni una misura che prevede il trattamento di siffatti dati possa essere adottata, garantendo così che l'ingerenza sia limitata allo stretto necessario.

94. È sulla base di tali principi che procederò all'analisi delle questioni pregiudiziali.

## **E. Risposta alle questioni pregiudiziali**

### **1. Sulla prima questione pregiudiziale**

95. Con la prima questione, 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 nonché dell'articolo 52, paragrafo 1, della Carta, osti a una normativa che:

- prevede un obbligo per i fornitori di servizi di comunicazione elettronica di conservare e di trattare i dati relativi al traffico oggetto di tale normativa, per un periodo di quattro o dodici mesi, a seconda dei casi, affinché tali fornitori adottino le misure appropriate, proporzionate, preventive e riparatorie per impedire le frodi e gli usi illeciti delle loro reti ed evitare di arrecare danni agli utenti finali o di infastidirli, e per accertare le frodi o gli usi illeciti della rete o del servizio o poterne identificare l'autore e l'origine;
- consente ai fornitori di servizi di comunicazione elettronica di conservare e di trattare i dati relativi al traffico considerati oltre i termini suindicati, in caso di frode o di uso illecito specifico della rete accertato, per il tempo necessario alla sua analisi e alla sua soluzione o per il tempo necessario al trattamento di tale uso illecito;
- consente ai fornitori di servizi di comunicazione elettronica, senza prevedere l'obbligo di richiesta di un parere preventivo o di notifica a un'autorità indipendente, di conservare e trattare altri dati, diversi da quelli menzionati da tale direttiva, al fine di accertare la frode o l'uso illecito della rete o del servizio, o di identificarne l'autore e l'origine;

– consente ai fornitori di servizi di comunicazione elettronica, senza prevedere l'obbligo di richiesta di un parere preventivo o di notifica a un'autorità indipendente, di conservare e di trattare per un periodo di dodici mesi i dati relativi al traffico che ritengano necessari per garantire la sicurezza e il buon funzionamento delle loro reti e dei loro servizi di comunicazione elettronica, e in particolare per accertare e analizzare un attentato potenziale o reale a tale sicurezza, compreso l'accertamento dell'origine di tale attentato e, in caso di attentato specifico a detta sicurezza, di conservare tali dati per l'arco di tempo necessario al trattamento di detto attentato.

96. La prima questione pregiudiziale riguarda quindi l'articolo 122, § 4 e § 4/1, della legge del 13 giugno 2005. Tale disposizione prevede sia un obbligo sia una facoltà, imposti ai fornitori di servizi di comunicazione elettronica, di conservare un certo numero di dati relativi al traffico e all'ubicazione al fine di individuare o di identificare l'autore di una frode o di un uso illecito della rete o del servizio.

97. Il governo belga sostiene l'idea secondo cui una siffatta normativa è giustificata dall'obiettivo enunciato all'articolo 15, paragrafo 1, della direttiva 2002/58, di prevenzione, ricerca, accertamento e perseguimento di usi non autorizzati del sistema di comunicazione elettronica, e che essa è inoltre strettamente proporzionata a tale obiettivo.

98. Così non è, a mio avviso, nel caso di specie.

99. Inizierò dal rilevare che i dati oggetto dell'articolo 122, § 4 e § 4/1, della legge del 13 giugno 2005 rappresentano un insieme particolarmente ampio di dati. In tale disposizione sono contemplati: gli identificativi dell'origine e della destinazione della comunicazione, le date e le ore precise di inizio e di fine della comunicazione, l'ubicazione delle apparecchiature terminali delle parti della comunicazione, il numero di telefono all'origine della comunicazione in entrata, l'indirizzo IP all'origine della comunicazione in entrata, la marcatura temporale e la porta utilizzata, le date e le ore precise della comunicazione in entrata, nonché tutti i dati necessari per garantire la sicurezza e il buon funzionamento delle reti e dei servizi di comunicazione elettronica. In tal senso, i dati conservati dai fornitori di servizi di comunicazione elettronica consentono di rintracciare e di individuare l'origine di una comunicazione e la destinazione di quest'ultima, di stabilire la data, l'ora, la durata, nonché l'ubicazione degli utenti ([49](#)). È quindi innegabile che tali dati consentono di trarre conclusioni precise sulla vita privata di tali utenti.

100. Anche se, secondo la mia lettura della giurisprudenza della Corte relativa all'articolo 15, paragrafo 1, della direttiva 2002/58, l'esistenza di una siffatta ingerenza nei diritti fondamentali può essere comunque giustificata sulla base di tale disposizione, ciò avviene solo a condizione che la normativa di cui trattasi imponga, per la conservazione di tale insieme di dati, un metodo di conservazione preciso in modo da limitare l'ingerenza derivante dalla conservazione di tale insieme di dati.

101. Orbene, dalla normativa nazionale non risulta affatto che i dati di cui trattasi siano conservati in condizioni e secondo modalità tecniche che garantiscano che sia escluso che ciò possa verificarsi. Infatti, essa non impone affatto modalità di conservazione di tali dati in modo da garantire una separazione effettivamente stagna di tali diverse categorie di dati che impedisca, nella fase di tale conservazione, qualsiasi utilizzo combinato delle diverse categorie di dati.

102. Pertanto, l'ingerenza determinata dalla conservazione dei dati di cui all'articolo 122, § 4 e § 4/1, della legge del 13 giugno 2005 non è, a mio avviso, proporzionata all'obiettivo perseguito.

103. In ogni caso, rilevo che la normativa di cui trattasi nel procedimento principale è caratterizzata, a mio avviso, da una grande incertezza sia quanto ai dati effettivamente conservati dai fornitori di servizi di comunicazione elettronica sia quanto alla durata di tale conservazione.

104. Infatti, da un lato, rilevo che, oltre ai dati espressamente elencati, l'articolo 122, § 4/1 della legge del 13 giugno 2005 consente ai fornitori di servizi di comunicazione elettronica di conservare «i dati relativi al traffico necessari per garantire la sicurezza e il buon funzionamento delle loro reti», e che esso prevede altresì che tali dati espressamente elencati possano essere integrati da un decreto regio.

105. D'altro lato, l'articolo 122, § 4 e § 4/1, di tale legge del 13 giugno 2005 autorizza parimenti i fornitori di servizi di comunicazione elettronica a conservare i dati di cui trattasi per il periodo necessario al trattamento di una frode o di un uso illecito della rete individuata, al di là della durata espressamente prevista dal legislatore.

106. In tal modo, spetta in definitiva ai fornitori di servizi di comunicazione elettronica decidere se procedere alla conservazione di dati, determinare la portata dei dati di cui trattasi e il periodo della loro conservazione.

107. Pertanto, in assenza di norme chiare e precise relative tanto alla portata dei dati conservati quanto alla durata della loro conservazione, lasciando aperta la possibilità di una conservazione illimitata su iniziativa esclusiva dei fornitori di servizi di comunicazione elettronica, la normativa nazionale di cui trattasi nel procedimento principale non può essere considerata proporzionata all'obiettivo perseguito.

108. Del pari, una siffatta normativa mi sembra manifestamente contraria al requisito secondo cui qualsiasi limitazione all'esercizio dei diritti fondamentali deve essere prevista dalla legge, il che implica che la base giuridica che consente l'ingerenza in tali diritti deve definire essa stessa la portata della limitazione dell'esercizio del diritto considerato ([50](#)).

109. Pertanto, ritengo che l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7 e 8 nonché dell'articolo 52, paragrafo 1, della Carta, debba essere interpretato nel senso che osta a una normativa nazionale come quella considerata dal giudice del rinvio nella sua prima questione pregiudiziale.

## 2. ***Sulla seconda questione pregiudiziale***

110. Con la seconda questione, 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 nonché dell'articolo paragrafo 1, della Carta osti a una normativa che:

- consente ai fornitori di servizi di comunicazione elettronica di conservare e di trattare i dati relativi all'ubicazione, senza che tale normativa descriva con precisione quali dati siano interessati, nell'ambito della fornitura di una rete o di un servizio in oggetto, per un periodo di quattro o dodici mesi, a seconda dei casi, quando sia necessario per il buon funzionamento e la sicurezza di tale rete o di tale servizio, o per accertare o analizzare le frodi o gli usi illeciti di detta rete;
- consente ai fornitori di servizi di comunicazione elettronica di conservare e di trattare i dati relativi all'ubicazione oltre i termini suindicati, in caso di attentato, di frode o di uso illecito specifico.

111. La seconda questione riguarda quindi l'articolo 123 della legge del 13 giugno 2005, che prevede l'obbligo per i fornitori di servizi di comunicazione elettronica di conservare i dati relativi all'ubicazione per un periodo di quattro o dodici mesi, a seconda dei casi, nonché la facoltà di prorogare tali termini di conservazione.

112. Tale questione fa riferimento alla conservazione dei dati relativi all'ubicazione diversi dai dati relativi al traffico. A tal riguardo ricordo, come enunciato dal considerando 35 della direttiva 2002/58, che i dati relativi all'ubicazione, che consentono di determinare la posizione geografica dell'apparecchiatura terminale dell'utente mobile, sono dati relativi al traffico di cui all'articolo 6 di tale direttiva quando sono trattati per consentire la trasmissione delle comunicazioni. Tuttavia, in aggiunta ad essi, le reti mobili digitali possono avere la capacità di trattare dati relativi all'ubicazione che possiedono un grado di precisione molto maggiore di quello necessario per la trasmissione delle comunicazioni e che vengono utilizzati per fornire servizi a valore aggiunto, come i servizi che forniscono informazioni individuali sul traffico e radioguida. Questo tipo di dati rientra nell'ambito di applicazione dell'articolo 9 di detta direttiva, il quale prevede che tali dati possano essere trattati solo in forma anonima oppure con il consenso degli utenti o degli abbonati ([51](#)).

113. Dato che la normativa nazionale di cui trattasi nel procedimento principale limita la portata dei diritti e degli obblighi previsti da tale disposizione, essa deve rispettare i requisiti previsti all'articolo 15, paragrafo 1, della medesima direttiva, come interpretato dalla giurisprudenza della Corte.

114. Rilevo che la normativa oggetto della seconda questione pregiudiziale presenta, a mio avviso, le stesse caratteristiche di quella oggetto della prima questione, caratteristiche che mi hanno portato a considerarla contraria all'articolo 15, paragrafo 1, della direttiva 2002/58.

115. Infatti, da un lato, essa non prevede alcun requisito di strutturazione dei dati e, dall'altro, manca di precisione sia per quanto riguarda i dati conservati sia per quanto riguarda la durata della loro conservazione, dato che questi due elementi sono lasciati alla discrezionalità dei fornitori di servizi di comunicazione elettronica.

116. Pertanto, per le stesse ragioni individuate nella mia risposta alla prima questione([52](#)), l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7 e 8 nonché dell'articolo 52, paragrafo 1, della Carta, deve essere interpretato nel senso che osta a una normativa nazionale come quella considerata dal giudice del rinvio nella sua seconda questione pregiudiziale.

### 3. Sulla terza questione pregiudiziale

117. Con la terza questione, il giudice del rinvio chiede, in sostanza, se, in caso di risposta affermativa alle prime due questioni pregiudiziali, esso possa mantenere temporaneamente gli effetti delle disposizioni della legge del 20 luglio 2022 incompatibili con il diritto dell'Unione, al fine di evitare una situazione di incertezza giuridica e di consentire che i dati raccolti e conservati in precedenza possano essere utilizzati conformemente agli obiettivi perseguiti da tale legge.

118. A tal riguardo, ricordo che la Corte ha risposto negativamente a una questione simile, in particolare, nella causa che ha dato luogo alla sentenza *Quadrature du Net I* ([53](#)). Non occorre, a mio avviso, pervenire ad un risultato diverso.

119. Pertanto, essa ha ricordato che il principio del primato del diritto dell'Unione sancisce la preminenza del diritto dell'Unione sul diritto degli Stati membri e impone quindi a tutte le istituzioni degli Stati membri di dare pieno effetto alle varie norme dell'Unione, dato che il diritto degli Stati membri non può sminuire l'efficacia riconosciuta a tali differenti norme nel territorio dei suddetti Stati ([54](#)). In forza di tale principio, ove non sia possibile procedere a un'interpretazione della normativa nazionale conforme alle prescrizioni del diritto dell'Unione, il giudice nazionale incaricato di applicare, nell'ambito di propria competenza, le disposizioni di diritto dell'Unione ha l'obbligo di garantire la piena efficacia delle medesime disapplicando all'occorrenza, di propria iniziativa, qualsiasi disposizione contrastante della legislazione nazionale, anche posteriore, senza doverne chiedere o attendere la previa rimozione in via legislativa o mediante qualsiasi altro procedimento costituzionale ([55](#)).

120. Solo la Corte può, eccezionalmente e per considerazioni imperative di certezza del diritto, concedere una sospensione provvisoria dell'effetto di disapplicazione esercitato da una norma di diritto dell'Unione rispetto a norme di diritto interno con essa in contrasto. Una siffatta limitazione nel tempo degli effetti dell'interpretazione data dalla Corte a tale diritto può essere concessa solo nella stessa sentenza che statuisce su tale interpretazione. Il primato e l'applicazione uniforme del diritto dell'Unione risulterebbero pregiudicati se i giudici nazionali avessero il potere di attribuire alle norme nazionali,

anche solo provvisoriamente, il primato rispetto al diritto dell'Unione al quale esse contravvengono (56).

121. Inoltre, secondo una giurisprudenza costante, l'interpretazione che la Corte dà di una norma di diritto dell'Unione, nell'esercizio della competenza attribuitale dall'articolo 267 TFUE, chiarisce e precisa il significato e la portata di tale norma, come deve o avrebbe dovuto essere intesa e applicata dal momento della sua entrata in vigore. Ne deriva che detta norma così interpretata può e deve essere applicata dal giudice anche a rapporti giuridici sorti e costituiti prima della pronuncia della sentenza che statuisce su tale domanda di interpretazione, purché sussistano, inoltre, i presupposti per sottoporre al giudice competente una controversia relativa all'applicazione di detta norma (57).

122. A tal riguardo, occorre ancora precisare che una limitazione nel tempo degli effetti dell'interpretazione adottata non è stata operata nelle sentenze *Tele2 Sverige et Watson e a.* (58), *Quadrature du Net I*, o ancora *Commissioner of An Garda Síochána e a.* (59), cosicché essa non può intervenire in una sentenza della Corte successiva a queste ultime.

123. In tali circostanze, ritengo che occorra rispondere alla terza questione pregiudiziale nel senso che il diritto dell'Unione osta a che un giudice nazionale applichi una disposizione di diritto nazionale che limita gli effetti nel tempo di una dichiarazione di invalidità ad esso incombente, in forza di tale diritto, nei confronti di una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica un obbligo di conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione incompatibile con 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.

## V. Conclusione

124. Alla luce di tutte le suesposte considerazioni, propongo alla Corte di rispondere alle questioni pregiudiziali sollevate dalla Cour constitutionnelle (Corte costituzionale, Belgio), dichiarando quanto segue:

1) l'articolo 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea,

deve essere interpretato nel senso che:

esso osta a una normativa nazionale che:

– prevede un obbligo per i fornitori di servizi di comunicazione elettronica di conservare e di trattare i dati relativi al traffico oggetto di tale normativa, per un periodo di quattro o dodici

mesi, a seconda dei casi, affinché essi adottino le misure appropriate, proporzionate, preventive e riparatorie per impedire le frodi e gli usi illeciti delle loro reti ed evitare di arrecare danni agli utenti finali o di infastidirli, e per accertare le frodi o gli usi illeciti della rete o del servizio o poterne identificare l'autore e l'origine;

- consente ai fornitori di servizi di comunicazione elettronica di conservare e di trattare i dati relativi al traffico considerati oltre i termini suindicati, in caso di frode o di uso illecito specifico della rete accertato, per il tempo necessario alla sua analisi e alla sua soluzione o per il tempo necessario al trattamento di tale uso illecito;
- consente ai fornitori di servizi di comunicazione elettronica, senza prevedere l'obbligo di richiesta di un parere preventivo o di notifica a un'autorità indipendente, di conservare e trattare altri dati, diversi da quelli menzionati da tale direttiva, al fine di accertare la frode o l'uso illecito della rete o del servizio, o di identificarne l'autore e l'origine;
- consente ai fornitori di servizi di comunicazione elettronica, senza prevedere l'obbligo di richiesta di un parere preventivo o di notifica a un'autorità indipendente, di conservare e di trattare per un periodo di dodici mesi i dati relativi al traffico che ritengano necessari per garantire la sicurezza e il buon funzionamento delle loro reti e dei loro servizi di comunicazione elettronica, e in particolare per accertare e analizzare un attentato potenziale o reale a tale sicurezza, compreso l'accertamento dell'origine di tale attentato e, in caso di attentato specifico a detta sicurezza, di conservare tali dati per l'arco di tempo necessario al trattamento di tale attentato.

2) L'articolo 15, paragrafo 1, di tale direttiva, letto alla luce degli articoli 7, 8 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali,

deve essere interpretato nel senso che:

esso osta a una normativa nazionale che:

- consente ai fornitori di servizi di comunicazione elettronica di conservare e di trattare i dati relativi all'ubicazione, senza che tale normativa descriva con precisione quali dati siano interessati, nell'ambito della fornitura di una rete o di un servizio, per un periodo di quattro o dodici mesi, a seconda dei casi, quando sia necessario per il buon funzionamento e la sicurezza di tale rete o di tale servizio, o per accertare o analizzare le frodi o l'uso illecito di detta rete;
- consente ai fornitori di servizi di comunicazione elettronica di conservare e di trattare i dati relativi all'ubicazione oltre i termini suindicati, in caso di attentato, di frode o di uso illecito specifico.

3) Il diritto dell'Unione deve essere interpretato nel senso che esso osta a che un giudice nazionale applichi una disposizione di diritto nazionale che limita gli effetti nel tempo di una dichiarazione di invalidità ad esso incombente, in forza di tale diritto, nei confronti di una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica

un obbligo di conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione incompatibile con l'articolo 15, paragrafo 1, della medesima direttiva, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali.

---

[1](#) Lingua originale: il francese.

---

[2](#) Sentenza n. 57/2021 del 22 aprile 2021 (ECLI:BE:GHCC:2021:AR.057).

---

[3](#) Sentenza del 6 ottobre 2020 (C-511/18, C-512/18 e C-520/18, in prosieguo la « sentenza La Quadrature du Net I », EU:C:2020:791).

---

[4](#) 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 »).

---

[5](#) Sentenza del 30 aprile 2024 (C-470/21, in prosieguo la « sentenza La Quadrature du Net II », EU:C:2024:370).

---

[6](#) 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).

---

[7](#) GU 2002, L 108, pag. 33.

---

[8](#) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU 2016, L 119, pag. 1; in prosieguo: il « RGPD »).

---

[9](#) Direttiva del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU 2016, L 119, pag. 89).

---

10 Sentenze La Quadrature du Net I, punto 107), del 5 aprile 2022, [Commissioner of An Garda Síochána e a.](#) (C-140/20, EU:C:2022:258, punto 35) nonché del 20 settembre 2022, [SpaceNet e Telekom Deutschland](#) (C-793/19 e C-794/19, EU:C:2022:702, punto 52).

---

11 Sentenze del 21 dicembre 2016, [Tele2 Sverige e Watson e a.](#) (C-203/15 e C-698/15, EU:C:2016:970, punto 86), La Quadrature du Net I (punto 108), del 5 aprile 2022, [Commissioner of An Garda Síochána e a.](#) (C-140/20, EU:C:2022:258, punto 38) nonché del 20 settembre 2022, [SpaceNet e Telekom Deutschland](#) (C-793/19 e C-794/19, EU:C:2022:702, punto 55).

---

12 Sentenze del 21 dicembre 2016, [Tele2 Sverige e Watson e a.](#) (C-203/15 e C-698/15, EU:C:2016:970, punto 86), La Quadrature du Net I (punto 108), del 5 aprile 2022, [Commissioner of An Garda Síochána e a.](#) (C-140/20, EU:C:2022:258, punto 38) nonché del 20 settembre 2022, [SpaceNet e Telekom Deutschland](#) (C-793/19 e C-794/19, EU:C:2022:702, punto 55).

---

13 Sentenze del 5 aprile 2022, [Commissioner of An Garda Síochána e a.](#) (C-140/20, EU:C:2022:258, punto 39) e del 20 settembre 2022, [SpaceNet e Telekom Deutschland](#) (C-793/19 e C-794/19, EU:C:2022:702, punto 56).

---

14 Sentenze La Quadrature du Net I (punto 112), del 5 aprile 2022, [Commissioner of An Garda Síochána e a.](#) (C-140/20, EU:C:2022:258, punto 41) e del 20 settembre 2022, [SpaceNet e Telekom Deutschland](#) (C-793/19 e C-794/19, EU:C:2022:702, punto 58), nonché [La Quadrature du Net II.](#) ( punto 67),

---

15 Sentenze La Quadrature du Net I, punti 110 e 111), del 5 aprile 2022, [Commissioner of An Garda Síochána e a.](#) (C-140/20, EU:C:2022:258, punto 40) nonché del 20 settembre 2022, [SpaceNet e Telekom Deutschland](#) (C-793/19 e C-794/19, EU:C:2022:702, punto 57).

---

16 Sentenze La Quadrature du Net I (punti da 120 a 122), del 5 aprile 2022, [Commissioner of An Garda Síochána e a.](#) (C-140/20, EU:C:2022:258, punti 48 e 49) nonché del 20 settembre 2022, [SpaceNet e Telekom Deutschland](#) (C-793/19 e C-794/19, EU:C:2022:702, punti 63 e 64).

---

17 Sentenze La Quadrature du Net I (punti da 127 a 129), del 5 aprile 2022, [Commissioner of An Garda Síochána e a.](#) (C-140/20, EU:C:2022:258, punti 50 e 51) nonché del 20 settembre 2022, [SpaceNet e Telekom Deutschland](#) (C-793/19 e C-794/19, EU:C:2022:702, punti 65 e 66).

---

18 (C-470/21, EU:C:2023:711, paragrafi 42 e 43).

---

19 Sentenza La Quadrature du Net I (punto 132).

---

[20](#) Sentenze La Quadrature du Net I, punto 131), del 5 aprile 2022, [Commissioner of An Garda Síochána e a.](#) (C-140/20, EU:C:2022:258, punto 53) nonché del 20 settembre 2022, [SpaceNet e Telekom Deutschland](#) (C-793/19 e C-794/19, EU:C:2022:702, punto 68).

---

[21](#) Sentenza del 20 settembre 2022, [SpaceNet e Telekom Deutschland](#) (C-793/19 e C-794/19, EU:C:2022:702, punto 71).

---

[22](#) Sentenza La Quadrature du Net I (punto 168).

---

[23](#) Sentenza del 21 dicembre 2016, [Tele2 Sverige e Watson e a.](#) (C-203/15 e C-698/15, EU:C:2016:970, punto 112).

---

[24](#) Sentenze dell'8 aprile 2014, [Digital Rights Ireland e a.](#) (C-293/12 e C-594/12, EU:C:2014:238, punto 59), e del 21 dicembre 2016, [Tele2 Sverige e Watson e a.](#) (C-203/15 e C-698/15, EU:C:2016:970, punto 108) nonché La Quadrature du Net I (punto 168).

---

[25](#) Sentenza La Quadrature du Net I (punto 168).

---

[26](#) Sentenza La Quadrature du Net I (punto 168).

---

[27](#) Corte EDU, 28 maggio 2024, Pietrzak e Bychawska-Siniardska e altri c. Polonia, CE:ECHR:2024:0528JUD007203817, punto 259.

---

[28](#) Corte EDU, 28 maggio 2024, Pietrzak e Bychawska-Siniardska e altri c. Polonia, CE:ECHR:2024:0528JUD007203817, punto 264.

---

[29](#) Sentenza La Quadrature du Net II.

---

[30](#) E non soltanto contro la criminalità grave, come era stato dichiarato nella sentenza La Quadrature du Net I.

---

[31](#) Sentenza La Quadrature du Net II (punto 83).

---

[32](#) Sentenza La Quadrature du Net II (punto 84).

---

[33](#) Sentenza La Quadrature du Net II (punto 85).

---

[34](#) La Corte enuncia una serie di condizioni idonee a garantire l'effettiva impermeabilità della separazione delle diverse categorie di dati conservati. V., a tal riguardo, sentenza La Quadrature du Net II (punti da 86 a 89). V. su tale punto, anche paragrafo 71 delle presenti conclusioni.

---

[35](#) Sentenze La Quadrature du Net I(punto 154), e sentenza La Quadrature du Net II (punto 117).

---

[36](#) Sentenza La Quadrature du Net II (punto 118).

---

[37](#) V., in tal senso, sentenza La Quadrature du Net II ( punto 119).

---

[38](#) Sentenza La Quadrature du Net II (punto 86).

---

[39](#) Sentenza La Quadrature du Net II ( punto 87).

---

[40](#) Sentenza La Quadrature du Net II ( punto 88).

---

[41](#) Sentenza La Quadrature du Net II (punto 89).

---

[42](#) Sentenze La Quadrature du Net I(punto 115) e La Quadrature du Net II ( punto 69).

---

[43](#) Sentenze La Quadrature du Net I( punto 116) e La Quadrature du Net II (punto 69).

---

[44](#) Sentenza del 21 dicembre 2016, [Tele2 Sverige e Watson e a.](#) (C-203/15 e C-698/15, EU:C:2016:970, punto 79).

---

[45](#) Sulla necessità della conservazione dei dati relativi al traffico e all'ubicazione in vista del loro successivo accesso, Eurojust and Europol, *Common Challenges in Cybercrime - 2024 Review by Eurojust and Europol*, Ufficio delle pubblicazioni dell'Unione europea, Lussemburgo, 2025, pag. 7.

---

[46](#) Sentenze dell'8 aprile 2014, [Digital Rights Ireland e a.](#) (C-293/12 e C-594/12, EU:C:2014:238, punto 59), e del 21 dicembre 2016, [Tele2 Sverige e Watson e a.](#) (C-203/15 e C-698/15, EU:C:2016:970, punto 108) nonché La Quadrature du Net I (punto 168).

---

[47](#) V., su tale punto, Dichiarazione congiunta dei capi di polizia europea del marzo 2023, (Indirizzo Internet: EDOC-#1384205-v1-Joint\_Declaration\_of\_the\_European\_Police\_Chiefs.PDF).

---

[48](#) Una siffatta soluzione mi sembra inoltre in linea con la giurisprudenza della Corte EDU che, rendendo la proporzionalità di una misura di conservazione dei dati il fulcro della sua analisi, consente proprio di tener conto delle eventuali garanzie poste in essere volte a limitare l'ingerenza che tale misura presuppone nei diritti degli utenti. V., in particolare, sulla necessità di istituire garanzie adeguate, Corte EDU, 28 maggio 2024, Pietrzak e Bychawska-Siniardska e altri c. Polonia, CE:ECHR:2024:0528JUD007203817, punti 250 e 251.

---

[49](#) Sentenza del 21 dicembre 2016, [Tele2 Sverige e Watson e a.](#) (C-203/15 e C-698/15, EU:C:2016:970, punto 98).

---

[50](#) Sentenze del e del 6 ottobre 2020, [Privacy International](#) (C-623/17, EU:C:2020:790, punto 65) e del 21 giugno 2022, [Ligue des droits humains](#) (C-817/19, EU:C:2022:491, punto 114).

---

[51](#) Sentenza del 21 dicembre 2016, [Tele2 Sverige e Watson e a.](#) (C-203/15 e C-698/15, EU:C:2016:970, punto 86).

---

[52](#) V., in particolare, paragrafi 99 e segg. delle presenti conclusioni.

---

[53](#) Sentenza La Quadrature du Net I (punti da 214 a 220).

---

[54](#) Sentenza La Quadrature du Net I (punto 214). V., altresì, sentenza del 5 aprile 2022, [Commissioner of An Garda Síochána e a.](#) (C-140/20, EU:C:2022:258, punto 118).

---

[55](#) Sentenze del 22 giugno 2010, [Melki e Abdeli](#) (C-188/10 e C-189/10, EU:C:2010:363, punto 43), La Quadrature du Net I (punto 215), nonché del 5 aprile 2022, [Commissioner of An Garda Síochána e a.](#) (C-140/20, EU:C:2022:258, punto 118).

---

[56](#) Sentenze La Quadrature du Net I (punti 216 e 217) nonché del 5 aprile 2022, [Commissioner of An Garda Síochána e a.](#) (C-140/20, EU:C:2022:258, punto 119).

---

[57](#) Sentenza del 5 aprile 2022, [Commissioner of An Garda Síochána e a.](#) (C-140/20, EU:C:2022:258, punto 125).

---

[58](#) Sentenza del 21 dicembre 2016 (C-203/15 e C-698/15, EU:C:2016:970).

---

[59](#) Sentenza del 5 aprile 2022 (C-140/20, EU:C:2022:258).