Causa C-511/18

Domanda di pronuncia pregiudiziale

Data di deposito:

3 agosto 2018

Giudice del rinvio:

Conseil d'État (Francia)

Data della decisione di rinvio:

26 luglio 2018

Ricorrenti:

La Quadrature du Net

French Data Network

Fédération des fournisseurs d'accès à Internet associatifs

Igwan.net

Resistenti:

Premier ministre

Garde des Sceaux, Ministre de la Justice

Ministre de l'Intérieur

Ministre des Armées

(omissis) Il Conseil d'État (Consiglio di Stato, Francia), pronunciandosi in sede contenziosa

(omissis) (Sezione del contenzioso, Nona e Decima Sezione riunite)

(omissis)

1. Con numero di ruolo 394922, con ricorso sommario, memoria integrativa e tre altre memorie, registrati il 30 novembre 2015, il 29 febbraio e il 6 maggio 2016, il 13 novembre 2017 e il 10 luglio 2018 presso la segreteria della Sezione

contenzioso del Conseil d'État (Consiglio di Stato francese), La Quadrature du Net, la French Data Network e la Fédération des fournisseurs d'accès à internet associatifs chiedono al Conseil d'État (Consiglio di Stato):

1) di annullare per eccesso di potere il décret nº 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement (decreto n. 2015-1185 del 28 settembre 2015, recante designazione dei servizi d'informazione specializzati);

2) in subordine, di sottoporre alla Corte di giustizia dell'Unione europea una serie di questioni pregiudiziali;

3) (omissis).

Esse affermano quanto segue:

– (omissis) [motivo concernente la legittimità formale, respinto dal giudice del rinvio];

– le disposizioni legislative che costituiscono la base giuridica del decreto impugnato violano il diritto al rispetto della vita privata e il diritto a un ricorso effettivo, garantiti rispettivamente dagli articoli 8 e 13 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e, di conseguenza, tale decreto è privo di fondamento giuridico;

– le disposizioni legislative che costituiscono la base giuridica del decreto impugnato violano il diritto al rispetto della vita privata, il diritto alla protezione dei dati di carattere personale e il diritto a un ricorso effettivo garantiti, rispettivamente, dagli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea e, di conseguenza, tale decreto è privo di fondamento giuridico; **[Or. 2]**

– l'articolo L. 851-3 del code de la sécurité intérieure (codice della sicurezza interna), che costituisce la base giuridica del decreto controverso, viola la direttiva 2000/31/CE, dell'8 giugno 2000, e, di conseguenza, tale decreto è privo di fondamento giuridico;

– il decreto impugnato deve essere ritenuto privo di fondamento giuridico in ragione dell'incompatibilità dell'articolo 323-8 del code pénal (codice penale) con gli articoli 6 e 32 della Convenzione sulla criminalità informatica, del 23 novembre 2001, con gli articoli 8 e 13 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e con il primo protocollo addizionale a tale convenzione e, per l'effetto, tale decreto è privo di fondamento giuridico.

Con due memorie difensive, registrate il 26 aprile e il 4 luglio 2016, il Ministre de la défense (Ministro della Difesa) chiede che il ricorso sia respinto. A suo giudizio, i motivi dedotti sarebbero infondati.

Con tre memorie difensive, registrate il 27 giugno 2016 e il 26 e il 28 giugno 2018, il Premier ministre (Primo ministro, Francia) chiede che il ricorso sia respinto. Egli afferma che i motivi dedotti sono infondati.

2. Con numero di ruolo 394925, con ricorso sommario, memoria integrativa e tre altre memorie, registrati il 30 novembre 2015, il 29 febbraio e il 6 maggio 2016, il 13 novembre 2017 e il 10 luglio 2018 presso la segreteria della Sezione contenzioso del Conseil d'État (Consiglio di Stato), La Quadrature du Net, la French Data Network e la Fédération des fournisseurs d'accès à internet associatifs chiedono al Conseil d'État (Consiglio di Stato):

1) di annullare per eccesso di potere il décret nº 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (decreto n. 2015-1211, del 1° ottobre 2015, relativo al contenzioso in materia di attuazione delle tecniche di informazione soggette ad autorizzazione e di fascicoli concernenti la sicurezza dello Stato);

2) in subordine, di sottoporre alla Corte di giustizia dell'Unione europea una serie di questioni pregiudiziali;

3) (omissis).

Esse affermano quanto segue:

– (omissis);

– le disposizioni legislative che costituiscono la base giuridica del decreto impugnato violano il diritto al rispetto della vita privata e il diritto a un ricorso effettivo, garantiti rispettivamente dagli articoli 8 e 13 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e, di conseguenza, tale decreto è privo di fondamento giuridico;

– le disposizioni legislative che costituiscono la base giuridica del decreto impugnato violano il diritto al rispetto della vita privata, il diritto alla protezione dei dati di carattere personale e il diritto a un ricorso effettivo garantiti, rispettivamente, dagli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea e, di conseguenza, tale decreto è privo di fondamento giuridico;

– l'articolo L. 851-3 del code de la sécurité intérieure (codice della sicurezza interna), che costituisce la base giuridica del decreto controverso, viola la direttiva 2000/31/CE, dell'8 giugno 2000, e, di conseguenza, tale decreto è privo di fondamento giuridico. **[Or. 3]**

Con memoria difensiva, registrata il 13 giugno 2016, il Garde des Sceaux, Ministre de la Justice (Ministro guardasigilli della Giustizia, Francia), chiede il rigetto del ricorso. Egli afferma che il ricorso è irricevibile in quanto le

associazioni non dimostrano di vantare un interesse tale da attribuire loro la legittimazione ad agire e che, in ogni caso, i motivi dedotti sono infondati.

Con tre memorie difensive, registrate il 27 giugno 2016 e il 26 e il 28 giugno 2018, il Primo ministro chiede che il ricorso sia respinto. Egli afferma che i motivi dedotti sono infondati.

3. Con numero di ruolo 397844, con ricorso sommario, memoria integrativa e altre due memorie, registrati l'11 marzo 2016, il 6 maggio 2016, il 13 novembre 2017 e il 10 luglio 2018, presso la segreteria del contenzioso del Conseil d'État (Consiglio di Stato), l'associazione Igwan.net chiede al Conseil d'État (Consiglio di Stato):

1) di annullare per eccesso di potere il décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure (decreto n. 2015-1639, dell'11 dicembre 2015, relativo alla designazione dei servizi diversi dai servizi di informazione specializzati, autorizzati a utilizzare le tecniche di cui al titolo V del libro VIII del codice della sicurezza interna, adottato in applicazione dell'articolo L. 811-4 del medesimo codice);

2) in subordine, di sottoporre alla Corte di giustizia dell'Unione europea una serie di questioni pregiudiziali;

3) (omissis).

Essa afferma quanto segue:

– (omissis);

– le disposizioni legislative che costituiscono la base giuridica del decreto impugnato violano il diritto al rispetto della vita privata e il diritto a un ricorso effettivo, garantiti rispettivamente dagli articoli 8 e 13 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e, di conseguenza, tale decreto è privo di fondamento giuridico;

– le disposizioni legislative che costituiscono la base giuridica del decreto impugnato violano il diritto al rispetto della vita privata, il diritto alla protezione dei dati di carattere personale e il diritto a un ricorso effettivo garantiti, rispettivamente, dagli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea e, di conseguenza, tale decreto è privo di fondamento giuridico;

– l'articolo L. 851-3 del code de la sécurité intérieure (codice della sicurezza interna), che costituisce la base giuridica del decreto controverso, viola la

direttiva 2000/31/CE, dell'8 giugno 2000, e, di conseguenza, tale decreto è privo di fondamento giuridico.

Con due memorie difensive, registrate il 28 giugno 2016 e il 26 giugno 2018, il Ministre de l'intérieur (Ministro dell'Interno, Francia) chiede che il ricorso sia respinto. Egli afferma che il ricorso è irricevibile in quanto l'associazione non dimostra un interesse tale da attribuirle la legittimazione ad agire e, in subordine, che i motivi dedotti sono infondati. **[Or. 4]**

Con tre memorie difensive, registrate il 5 luglio 2016, il 26 e il 28 giugno 2018, il Primo ministro chiede che il ricorso sia respinto. Egli afferma che i motivi dedotti sono infondati.

4. Con numero di ruolo 397851, con ricorso sommario, memoria integrativa e due ulteriori memorie, registrati l'11 marzo 2016, il 19 maggio 2016, il 24 novembre 2017 e il 10 luglio 2018 presso la segreteria del contenzioso del Conseil d'État (Consiglio di Stato), La Quadrature du Net, la French Data Network e la Fédération des fournisseurs d'accès à internet associatifs chiedono al Conseil d'État (Consiglio di Stato):

1) di annullare per eccesso di potere il décret nº 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (decreto n. 2016-67, del 29 gennaio 2016, in materia di tecniche di raccolta di informazioni);

2) in subordine, di sottoporre alla Corte di giustizia dell'Unione europea una serie di questioni pregiudiziali;

3) (omissis).

Esse affermano quanto segue:

– (omissis);

– le disposizioni legislative che costituiscono la base giuridica del decreto impugnato sono state dichiarate incostituzionali dal Conseil constitutionnel (Consiglio costituzionale, Francia) e, di conseguenza, tale decreto è privo di fondamento giuridico;

– le disposizioni legislative che costituiscono la base giuridica del decreto impugnato violano il diritto al rispetto della vita privata e il diritto a un ricorso effettivo, garantiti rispettivamente dagli articoli 8 e 13 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e, di conseguenza, tale decreto è privo di fondamento giuridico;

– le disposizioni legislative che costituiscono la base giuridica del decreto impugnato violano il diritto al rispetto della vita privata, il diritto alla protezione dei dati di carattere personale e il diritto a un ricorso effettivo garantiti, rispettivamente, dagli articoli 7, 8 e 47 della Carta dei diritti

fondamentali dell'Unione europea e, di conseguenza, tale decreto è privo di fondamento giuridico;

– l'articolo L. 851-3 del code de la sécurité intérieure (codice della sicurezza interna), che costituisce la base giuridica del decreto controverso, viola la direttiva 2000/31/CE, dell'8 giugno 2000, e, di conseguenza, tale decreto è privo di fondamento giuridico;

– il decreto controverso viola le disposizioni degli articoli da L. 851-1 a L. 851-3 del codice della sicurezza interna, per la cui attuazione in particolare esso è stato adottato, ampliando il novero dei dati di connessione suscettibili di raccolta.

Con memoria difensiva registrata il 26 giugno 2018, il Ministro dell'Interno chiede il rigetto del ricorso. Egli afferma che i motivi dedotti sono infondati.

Con tre memorie difensive, registrate il 4 luglio 2016 e il 26 e il 28 giugno 2018, il Primo ministro chiede che il ricorso sia respinto. Egli afferma che i motivi dedotti sono infondati. **[Or. 5]**

Visti:

– la Constitution (Costituzione), in particolare il preambolo e gli articoli 61-1 e 62;

– il Trattato sull'Unione europea;

– il Trattato sul funzionamento dell'Unione europea;

– la Carta dei diritti fondamentali dell'Unione europea;

– la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali;

– la Convenzione sulla criminalità informatica, del 23 novembre 2001;

– la direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000;

– la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002;

– il codice della sicurezza interna, in particolare il libro VIII;

– la decisione del Conseil constitutionnel (Consiglio costituzionale) n. 2016-590 QPC, del 21 ottobre 2016;

– il code de justice administrative (codice di giustizia amministrativa);

(omissis);

Considerato quanto segue:

1. Con tre ricorsi, La Quadrature du Net, la French Data Network e la Fédération des fournisseurs d'accès à internet associatifs chiedono, rispettivamente, l'annullamento per eccesso di potere, con numero di ruolo 394922, del decreto del 28 settembre 2015, recante designazione dei servizi di informazione specializzati, con numero di ruolo 394925, del decreto del 1º ottobre 2015, relativo al contenzioso in materia di applicazione delle tecniche di informazione soggette ad autorizzazione e di fascicoli concernenti la sicurezza dello Stato, e, con numero di ruolo 397851, del decreto del 29 gennaio 2016, in materia di tecniche di raccolta di informazioni. Con numero di ruolo 397844, l'associazione Igwan.net chiede l'annullamento del decreto dell'11 dicembre 2015, relativo alla designazione dei servizi diversi dai servizi di informazione specializzati, autorizzati a utilizzare le tecniche di cui al titolo V del libro VIII del codice della sicurezza interna, adottato in applicazione dell'articolo L. 811-4 del medesimo codice. Tali ricorsi sollevano le medesime questioni. Essi devono pertanto essere riuniti al fine di adottare una decisione unitaria.

Sui motivi concernenti la legittimità formale:

2. (omissis) **[Or. 6]** (omissis). [motivi respinti dal giudice del rinvio] (omissis)

Sui motivi di legittimità sostanziale:

Sul motivo concernente la violazione dell'articolo L. 851-1 del codice della sicurezza interna da parte del decreto del 29 gennaio 2016, in materia di tecniche di raccolta di informazioni:

3. (omissis). [motivo respinto dal giudice del rinvio]

Per quanto riguarda i motivi dedotti mediante eccezione:

4. A sostegno delle domande formulate, le ricorrenti invocano, in via di eccezione, motivi contro tutte le disposizioni del libro VIII del codice della sicurezza interna, contro le disposizioni del capo III bis del titolo VU del libro VII del codice di giustizia amministrativa e contro quelle dell'articolo 323-8 del codice penale.

Per quanto riguarda il motivo concernente l'incostituzionalità dell'articolo L. 811-5 del codice della sicurezza interna:

5. (omissis) **[Or. 7]** (omissis). [Il giudice del rinvio ritiene che la dichiarazione di incostituzionalità dell'articolo L. 811-5 del codice della sicurezza interna [con decisione del Conseil constitutionnel (Consiglio costituzionale) del 21 ottobre 2016] non rilevi ai fini della conclusione delle presenti controversie]

Per quanto concerne l'eccezione di incompatibilità con le convenzioni internazionali sollevata nei confronti dell'articolo 323-8 del codice penale:

6. (omissis). [motivo respinto dal giudice del rinvio]

Per quanto riguarda i motivi concernenti la violazione della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali:

7. In primo luogo, le associazioni ricorrenti affermano che, viste le violazioni del diritto di ricorso, dei diritti della difesa e del principio del contraddittorio nel contesto del contenzioso in materia di applicazione delle tecniche di informazione, i decreti impugnati sono stati adottati sulla base o in applicazione di disposizioni legislative che violano il diritto a un ricorso effettivo garantito, segnatamente, dall'articolo 13 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

8. Le disposizioni degli articoli L. 841-1 e L. 841-2 del codice della sicurezza interna stabiliscono le condizioni in cui il Conseil d'État (Consiglio di Stato) è competente a conoscere di ricorsi concernenti l'applicazione delle tecniche di informazione soggette ad autorizzazione. Il Conseil d'État (Consiglio di Stato) può essere adito da chiunque intenda sincerarsi del fatto che nessuna tecnica di spionaggio è applicata in maniera irregolare e che dimostri di aver preliminarmente adito la Commission nationale de contrôle des techniques de renseignement (Commissione nazionale di controllo delle tecniche di informazione, Francia) sulla base dell'articolo L. 833-4 di detto codice, oppure dal presidente di detta commissione o da tre suoi membri, allorquando il Primo ministro non dà seguito ai pareri o alle raccomandazioni di detta commissione o adotti provvedimenti ritenuti insufficienti. Per quanto concerne le misure di controllo delle comunicazioni elettroniche internazionali disciplinate dal capo IV del titolo V del libro VIII del codice della sicurezza interna, la persona che ritiene di essere oggetto di una misura siffatta, pur non potendo adire direttamente un giudice per **[Or. 8]** contestarne la regolarità, può per contro, sulla base delle disposizioni dell'articolo L. 854-9 di detto codice, presentare a tal fine un reclamo dinanzi alla Commissione nazionale di controllo delle tecniche di informazione. Orbene, questo stesso articolo prevede che la commissione, ove, di propria iniziativa o a seguito di un reclamo siffatto, individui una violazione, trasmette una raccomandazione al Primo ministro volta a far sì che sia posta fine a detta violazione e che le informazioni raccolte siano, se del caso, distrutte. Essa può anche agire dinanzi al Conseil d'État (Consiglio di Stato).

9. Ove sia chiesta una pronuncia diretta a garantire che non vengano applicate, in modo irregolare tecniche di informazione nei confronti del ricorrente o dell'interessato, compete alla Sezione specializzata, istituita con l'articolo L 773-2 del codice di giustizia amministrativa verificare, alla luce degli elementi che le sono stati comunicati al di fuori della procedura in contraddittorio, se il ricorrente sia o meno oggetto di una tecnica siffatta. In caso affermativo, spetta a tale Sezione valutare se tale tecnica sia attuata in conformità al libro VIII del codice

della sicurezza interna. Ove emerga che nei confronti del ricorrente non è stata applicata alcuna tecnica di spionaggio o che detta applicazione non è in alcun modo illecita, la Sezione informa il ricorrente dell'avvenuto compimento di dette verifiche e della mancata commissione di illeciti, senza fornire ulteriori precisazioni. Ove sia stata applicata una tecnica di spionaggio in condizioni che appaiono illecite, essa ne informa il ricorrente, senza menzionare alcun elemento protetto dal segreto della difesa nazionale. In tal caso, mediante separata decisione, diretta unicamente all'amministrazione competente e alla Commissione nazionale di controllo delle tecniche di informazione, la Sezione specializzata annulla, se del caso, l'autorizzazione e ordina la distruzione delle informazioni raccolte in maniera irregolare.

10. La deroga prevista dalle contestate disposizioni del codice di giustizia amministrativa al carattere contraddittorio della procedura giudiziaria, che ha come unico scopo di informare i giudici di elementi coperti dal segreto della difesa nazionale e che, pertanto, non possono essere comunicati al ricorrente, permette alla Sezione specializzata, che sente le parti, di statuire con piena cognizione di causa. I poteri ad essa conferiti di istruire i ricorsi, rilevare d'ufficio ogni illecito da essa constatato e ordinare all'amministrazione di adottare tutte le misure utili per far fronte agli illeciti accertati, garantiscono l'effettività del controllo giurisdizionale da essa espletato.

11. Ne consegue che, contrariamente a quanto sostenuto, né le condizioni alle quali la Sezione specializzata può essere adita né quelle in cui essa esercita le sue funzioni giurisdizionali violano il diritto a un ricorso effettivo riconosciuto alle persone che si rivolgono ad essa, come garantito, in particolare, dall'articolo 13 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

12. In secondo luogo, le associazioni ricorrenti sostengono che i decreti impugnati sono stati adottati sulla base o in applicazione di disposizioni legislative che violano il diritto al rispetto della vita privata garantito, segnatamente, dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, in ragione della mancata notifica agli interessati delle misure di sorveglianza, una volta revocate.

13. Tenuto conto, da una parte, delle competenze affidate alla Commissione nazionale di controllo delle tecniche di informazione, un'autorità amministrativa indipendente cui spetta verificare, sotto il controllo del giudice, che le tecniche di raccolta delle informazioni siano applicate, sul territorio nazionale, nel rispetto degli obblighi risultanti dal codice **[Or. 9]** della sicurezza interna, e, dall'altra, del ricorso effettivo ammesso secondo le condizioni descritte ai punti che precedono dinanzi alla sezione specializzata dal Conseil d'État (Consiglio di Stato), il fatto che le disposizioni legislative contestate non prevedano la notifica agli interessati delle misure di sorveglianza cui sono stati sottoposti, una volta che esse sono state revocate, non integra, di per sé, una violazione eccessiva del diritto al rispetto della vita privata.

14. Alla luce di quanto precede, i motivi concernenti la contrarietà delle disposizioni legislative contestate agli articoli 8 e 13 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali devono, in ogni caso, essere respinti.

Sul motivo concernente la violazione della direttiva dell'8 giugno 2000

15. Le disposizioni dell'articolo L. 851-3 del codice della sicurezza interna permettono di imporre agli operatori di comunicazioni elettroniche e ai prestatori di servizi tecnici *«l'attuazione sulle loro reti di trattamenti automatizzati destinati, in funzione di parametri specificati nell'autorizzazione, a individuare collegamenti in grado di rivelare una minaccia terroristica»*. Questa tecnica è destinata unicamente a raccogliere, per un periodo limitato, tra tutti i dati di connessione trattati da tali soggetti, quelli che potrebbero presentare un legame con un siffatto grave reato. In tali circostanze, le disposizioni di cui trattasi, che non impongono un obbligo generale di sorveglianza attiva, non violano il chiaro disposto dell'articolo 15 della direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno, secondo cui, *«nella prestazione dei servizi di semplice trasporto, memorizzazione e hosting, gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite»*. Ne consegue che, in ogni caso, il motivo vertente sulla violazione della direttiva dell'8 giugno 2000 dev'essere respinto.

Sui motivi vertenti sulla violazione della direttiva del 12 luglio 2002 e della Carta dei diritti fondamentali dell'Unione europea:

16. Da una parte, a norma dell'articolo 4 del Trattato sull'Unione europea, l'Unione *«rispetta le funzioni essenziali dello Stato, in particolare le funzioni di salvaguardia dell'integrità territoriale, di mantenimento dell'ordine pubblico e di tutela della sicurezza nazionale. In particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro»*. L'articolo 51 della Carta dei diritti fondamentali dell'Unione europea prevede che: *«1. Le disposizioni della presente Carta si applicano alle istituzioni, organi e organismi dell'Unione nel rispetto del principio di sussidiarietà, come pure agli Stati membri esclusivamente nell'attuazione del diritto dell'Unione. (...) 2. La presente Carta non estende l'ambito di applicazione del diritto dell'Unione al di là delle competenze dell'Unione, né introduce competenze nuove o compiti nuovi per l'Unione, né modifica le competenze e i compiti definiti nei trattati»*. A norma del suo articolo 54, *«Nessuna disposizione della presente Carta deve essere interpretata nel senso di comportare il diritto di esercitare un'attività o compiere un atto che miri a distruggere diritti o libertà riconosciuti nella presente Carta o a imporre a tali diritti e libertà limitazioni più ampie di quelle previste dalla presente Carta (...)»*.

17. Dall'altra, la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela **[Or. 10]** della vita privata nel settore delle comunicazioni elettroniche, adottata sulla base dell'articolo 95 del Trattato che istituisce la Comunità europea, ora ripreso nell'articolo 114 del Trattato sul funzionamento dell'Unione europea, nasce dalla volontà di ravvicinare le legislazioni degli Stati membri per permettere l'instaurazione e il funzionamento del mercato interno. Essa ha ad oggetto, come sancisce il suo articolo 3, paragrafo 1, il *«trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nella Comunità»*. Tuttavia, come ricorda il suo articolo 1, paragrafo 3, essa *«non si applica alle attività che esulano dal campo di applicazione del trattato che istituisce la Comunità europea (...) né, comunque, alle attività riguardanti la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) o alle attività dello Stato in settori che rientrano nel diritto penale»*. Peraltro, a norma del suo articolo 15, *«gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea»*. Gli Stati membri sono così autorizzati, per motivi attinenti alla sicurezza dello Stato o alla lotta alla criminalità, a derogare, in particolare, all'obbligo di riservatezza dei dati personali e dei relativi dati sul traffico risultanti dall'articolo 5, paragrafo l, della direttiva.

<u>Sull'ambito di applicazione dell'articolo 15, paragrafo 1, della direttiva del 12 luglio 2002:</u>

18. Dalle succitate disposizioni della direttiva del 12 luglio 2002, come statuito dalla Corte di giustizia dell'Unione europea nella sua sentenza *Tele2 Sverige AB/Post-och telestyrelsen e Secretary of State for the Home Department/Tom Watson e a.* (C-203/15 e C-698/15), del 21 dicembre 2016, si evince che essa «deve essere considerata come disciplinante le attività dei fornitori di tali servizi [di comunicazione elettronica]». Le disposizioni che prevedono obblighi a carico di detti fornitori, come la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione dei loro utenti e abbonati, per le finalità indicate all'articolo 15, paragrafo 1, della direttiva del 12 luglio 2002, tra cui rientra la salvaguardia della sicurezza nazionale, della difesa e della sicurezza

pubblica, ricadono quindi nell'ambito di applicazione di tale direttiva nella misura in cui, come stabilito dalla Corte di giustizia, disciplinano la loro attività. Inoltre, come stabilito sempre dalla Corte, il fatto che tali obblighi operino unicamente al fine di mettere a disposizione delle autorità nazionali competenti i dati personali che le riguardano comporta che la normativa nazionale disciplinante l'accesso e l'uso di tali dati rientri parimenti nel campo di applicazione della direttiva del 12 luglio 2002. Per contro, le disposizioni nazionali concernenti le tecniche di raccolta di informazioni attuate direttamente dallo Stato, senza disciplinare le attività dei fornitori di servizi di comunicazione elettronica imponendo loro obblighi specifici, non rientrano nell'ambito di applicazione della direttiva di cui trattasi. **[Or. 11]**

19. L'articolo L. 851-1 del codice della sicurezza interna così dispone: «*In conformità alle condizioni previste nel capo 1 del titolo II del presente libro, può essere autorizzata la raccolta, in capo agli operatori del settore delle comunicazioni elettroniche, ai soggetti indicati all'articolo L. 34-1 del code des postes et des communications électroniques [codice delle poste e delle comunicazioni elettroniche] e a quelli menzionati ai punti 1 e 2 dell'articolo 6 della loi n. 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [legge n. 2004-575 del 21 giugno 2004, in materia di promozione della fiducia nell'economia digitale], delle informazioni o dei documenti trattati o conservati attraverso le loro reti o servizi di comunicazione elettronica, ivi compresi i dati tecnici relativi all'identificazione dei numeri di abbonamento o di connessione ai servizi di comunicazione elettronica, al censimento di tutti i numeri di abbonamento o di connessione di una determinata persona, all'ubicazione delle apparecchiature terminali utilizzate nonché alle comunicazioni di un abbonato concernenti l'elenco dei numeri chiamati e chiamanti, la durata e la data delle comunicazioni (...)*». Gli articoli L. 851-2 e L. 851-4 del codice della sicurezza interna disciplinano, per finalità e secondo metodi differenti, gli accessi amministrativi in tempo reale ai dati di connessione così conservati.

20. Tenuto conto dell'ambito di applicazione dell'articolo 15, paragrafo 1, della direttiva del 12 luglio 2002, come interpretato dalla Corte di giustizia dell'Unione europea, da quanto precede risulta chiaramente che vi rientrano sia l'obbligo di conservazione derivante dalle succitate disposizioni dell'articolo L 851-1 del codice della sicurezza interna, sia gli accessi amministrativi ai dati di connessione, compresi quelli in tempo reale, che lo giustificano, di cui agli articoli L. 851-1, L. 851-2 e L. 851-4 del medesimo codice. Lo stesso vale per le disposizioni dell'articolo L. 851-3 del codice della sicurezza interna che, pur non prevedendo a carico degli operatori e degli interessati un obbligo preventivo di conservazione, tuttavia impongono loro di attuare sulle proprie reti trattamenti automatizzati intesi a identificare collegamenti idonei a rivelare una minaccia terroristica.

21. Per contro, dalla direttiva del 12 luglio 2002 risulta chiaramente che non rientrano nel suo ambito di applicazione le disposizioni degli articoli L. 851-5 e L. 851-6, né quelle dei capi II, III e IV del titolo V del libro VIII del codice della

sicurezza interna, in quanto riguardano tecniche di raccolta di informazioni che sono attuate direttamente dallo Stato senza disciplinare le attività dei fornitori di servizi di comunicazione elettronica imponendo loro obblighi specifici. Pertanto, dette disposizioni non possono essere considerate come attuative del diritto dell'Unione europea e, di conseguenza, i motivi vertenti sulla violazione della direttiva del 12 luglio 2002, interpretata alla luce della Carta dei diritti fondamentali dell'Unione europea, non possono essere validamente invocati nei loro confronti.

Sull'obbligo di conservazione generalizzata e indifferenziata:

22. Con sentenza del 21 dicembre 2016, la Corte di giustizia dell'Unione europea ha stabilito che l'articolo 15, paragrafo 1, di detta direttiva, «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 ad una normativa nazionale la quale preveda, per finalità di lotta contro la criminalità, una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica».

23. Da una parte, è pacifico che una siffatta conservazione preventiva e indifferenziata consente ai servizi di informazione di accedere ai dati relativi alle comunicazioni che una persona ha effettuato, prima che siano individuati i motivi che inducono a ritenere che essa integri una minaccia per la sicurezza pubblica, la difesa o la sicurezza dello Stato. In un **[Or. 12]** contesto segnato da gravi e persistenti minacce alla sicurezza nazionale, relative in particolare al rischio di terrorismo, una siffatta conservazione presenta un'utilità senza equivalenti rispetto alla raccolta di detti medesimi dati a partire soltanto dal momento in cui la persona in questione è stata individuata come in grado di presentare una minaccia per la sicurezza pubblica, la difesa o la sicurezza dello Stato.

24. Dall'altra, come osservato dalla Corte di giustizia dell'Unione europea nella sua sentenza del 21 dicembre 2016, una siffatta conservazione, nella misura in cui non svela il contenuto di una comunicazione, non è idonea a pregiudicare il «contenuto essenziale» dei diritti sanciti agli articoli 7 e 8 della Carta. Inoltre, la Corte ha successivamente ribadito, nel suo parere 1/15 del 26 luglio 2017, che tali diritti «non appaiono prerogative assolute» e che una finalità d'interesse generale dell'Unione può giustificare ingerenze, anche gravi, in detti diritti fondamentali, dopo aver osservato che «la protezione della sicurezza pubblica contribuisce altresì alla tutela dei diritti e delle libertà altrui» e che «l'articolo 6 della Carta enuncia il diritto di ogni persona non solo alla libertà, ma anche alla sicurezza».

25. Date le suddette circostanze, la questione di stabilire se, tenuto conto in particolare delle salvaguardie e dei controlli richiamati ai punti da 7 a 13, che accompagnano gli accessi amministrativi ai dati di connessione e il loro utilizzo, l'obbligo di conservazione generalizzata e indifferenziata, imposto ai fornitori sulla base delle disposizioni autorizzative di cui all'articolo 15, paragrafo 1, della

direttiva del 12 luglio 2002, non debba essere considerato come un'ingerenza giustificata dal diritto alla sicurezza garantito dall'articolo 6 della Carta dei diritti fondamentali dell'Unione europea e dalle esigenze di sicurezza nazionale, la cui responsabilità è rimessa, a norma dell'articolo 4 del Trattato sull'Unione europea, unicamente agli Stati membri, solleva un primo problema di interpretazione del diritto dell'Unione europea.

Sugli ulteriori obblighi che possono essere imposti ai fornitori di un servizio di comunicazione elettronica:

26. Le disposizioni dell'articolo L. 851-2 del codice della sicurezza interna autorizzano, esclusivamente al fine della prevenzione del terrorismo, la raccolta delle informazioni o dei documenti previsti all'articolo L. 851-1 in capo agli stessi soggetti. Tale raccolta, che riguarda unicamente una o più persone fisiche precedentemente identificate come potenzialmente collegate a una minaccia terroristica, è effettuato in tempo reale. Lo stesso vale per le disposizioni dell'articolo L. 851-4 di detto codice, che autorizzano la trasmissione in tempo reale, da parte degli operatori, dei soli dati tecnici concernenti l'ubicazione delle apparecchiature terminali. Ne consegue che tali tecniche non pongono a carico dei fornitori interessati un obbligo di conservazione aggiuntivo rispetto a quanto necessario ai fini della fatturazione e della commercializzazione dei loro servizi e alla fornitura di servizi a valore aggiunto. Inoltre, come ricordato al punto 15, le disposizioni dell'articolo L. 851-3 del codice della sicurezza interna non implicano nemmeno una conservazione generalizzata e indifferenziata.

27. Orbene, da una parte, è pacifico che gli accessi in tempo reale ai dati di connessione permettono di monitorare, con un elevato grado di reattività, i comportamenti di individui che possono rappresentare una minaccia attuale per l'ordine pubblico. Per contro, la tecnica prevista all'articolo L. 851-3 del codice della sicurezza interna consente di individuare, sulla base di criteri all'uopo precisamente definiti, i soggetti il cui comportamento, alla luce in particolare delle loro modalità di comunicazione, può rivelare una minaccia terroristica. In un contesto segnato da minacce gravi e persistenti alla sicurezza **[Or. 13]** nazionale, relative in particolare al rischio di terrorismo, tali tecniche presentano pertanto un'utilità dal punto di vista operativo senza equivalenti.

28. Dall'altra, come osservato dalla Corte di giustizia dell'Unione europea nella sua sentenza del 21 dicembre 2016, una siffatta conservazione, nella misura in cui non svela il contenuto di una comunicazione, non è idonea a pregiudicare il «contenuto essenziale» dei diritti sanciti agli articoli 7 e 8 della Carta. Inoltre, la Corte ha successivamente ribadito, nel suo parere 1/15 del 26 luglio 2017, che tali diritti «non appaiono prerogative assolute» e che una finalità d'interesse generale dell'Unione può giustificare ingerenze, anche gravi, in detti diritti fondamentali, dopo aver osservato che «la protezione della sicurezza pubblica contribuisce altresì alla tutela dei diritti e delle libertà altrui» e che «l'articolo 6 della Carta enuncia il diritto di ogni persona non solo alla libertà, ma anche alla sicurezza».

29. Date le circostanze, una seconda seria difficoltà di interpretazione del diritto dell'Unione europea è posta dalla questione di stabilire se la direttiva del 12 luglio 2002, letta alla luce della Carta dei diritti fondamentali dell'Unione europea, debba essere interpretata nel senso che essa autorizza misure legislative concernenti attività di pubblica sicurezza, difesa e sicurezza dello Stato, quali la raccolta in tempo reale di dati sul traffico e sull'ubicazione di persone determinate che, pur incidendo sui diritti e sugli obblighi dei fornitori di un servizio di comunicazioni elettroniche, non impongono loro uno specifico obbligo di conservazione dei loro dati.

Sull'accesso delle autorità nazionali competenti ai dati conservati:

30. Nella sua sentenza del 21 dicembre 2016, la Corte di giustizia dell'Unione europea ha inoltre stabilito che l'articolo 15, paragrafo 1, della direttiva del 12 luglio 2002, «deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale disciplini la protezione e la sicurezza dei dati relativi al traffico e dei dati relativi all'ubicazione, e segnatamente l'accesso delle autorità nazionali competenti ai dati conservati, senza limitare, nell'ambito della lotta contro la criminalità, tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre detto accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, e senza esigere che i dati di cui trattasi siano conservati nel territorio dell'Unione». In tale occasione, la Corte ha giudicato che «occorre che le autorità nazionali competenti alle quali è stato consentito l'accesso ai dati conservati ne diano notizia alle persone interessate, nell'ambito delle procedure nazionali applicabili, a partire dal momento in cui tale comunicazione non è suscettibile di compromettere le indagini condotte dalle autorità summenzionate. Infatti, tale informazione è, de facto, necessaria per consentire a dette persone di esercitare, in particolare, il diritto di ricorso, esplicitamente previsto dall'articolo 15, paragrafo 2, della direttiva 2002/58, letto in connessione con l'articolo 22 della direttiva 95/46, in caso di violazione dei loro diritti».

31. Una terza seria difficoltà di interpretazione del diritto dell'Unione è data dalla questione se la direttiva del 12 luglio 2002, letta alla luce della Carta dei diritti fondamentali dell'Unione europea, debba essere interpretata nel senso che essa subordina sempre la regolarità delle procedure di raccolta dei dati di connessione a un obbligo di informazione degli interessati, ove tale informazione non sia suscettibile di compromettere le indagini condotte dalle autorità competenti, o se tali procedure possano essere considerate regolari, tenuto conto di tutte le altre garanzie procedurali esistenti **[Or. 14]**, una volta che queste ultime garantiscono l'efficacia del diritto di ricorso.

32. Le tre questioni enunciate ai punti da 25 a 31 sono determinanti per l'esito delle controversie che il Conseil d'État (Consiglio di Stato) è chiamato a dirimere concernenti i quattro decreti impugnati, dal momento che essi sono stati adottati in attuazione degli articoli da L. 851-1 a L. 851-4 del codice della sicurezza interna. Esse presentano, come già osservato, molteplici serie difficoltà sotto il profilo

dell'interpretazione del diritto dell'Unione europea. È pertanto necessario adire la Corte di giustizia dell'Unione europea a norma dell'articolo 267 del Trattato sul funzionamento dell'Unione europea e sospendere, entro tali limiti, la decisione sui ricorsi proposti dalle associazioni ricorrenti sino alla pronuncia della Corte, respingendo, per il resto, le loro domande e senza che occorra pronunciarsi sulle eccezioni di irricevibilità sollevate in replica.

DECIDE:

Articolo 1: I ricorsi sono respinti nella parte in cui sono diretti avverso i decreti n. 2015-1185, del 28 settembre 2015, n. 2015-1211, del 1° ottobre 2015, n. 2015-1639, dell'11 dicembre 2015 e n. 2016-67, del 29 gennaio 2016, nella misura in cui attuano le disposizioni di cui agli articoli L. 851-5 e L. 851-6 e quelle di cui ai capi II, III e IV del titolo V del libro VIII del codice della sicurezza interna.

Articolo 2: La decisione sui ricorsi proposti dalle associazioni ricorrenti è sospesa, entro tali limiti, sino a quando la Corte di giustizia dell'Unione europea si sarà pronunciata sulle seguenti questioni:

1) Se l'obbligo di conservazione generalizzata e indifferenziata, imposto ai fornitori sulla base delle disposizioni autorizzative di cui all'articolo 15, paragrafo 1, della direttiva del 12 luglio 2002, debba essere considerato, in un contesto caratterizzato da minacce gravi e persistenti alla sicurezza nazionale, e in particolare dal rischio terroristico, come un'ingerenza giustificata dal diritto alla sicurezza garantito dall'articolo 6 della Carta dei diritti fondamentali dell'Unione europea e dalle esigenze di sicurezza nazionale, la cui responsabilità è rimessa, a norma dell'articolo 4 del Trattato sull'Unione europea, unicamente agli Stati membri.

2) Se la direttiva del 12 luglio 2002, letta alla luce della Carta dei diritti fondamentali dell'Unione europea, debba essere interpretata nel senso che essa autorizza misure legislative, quali la raccolta in tempo reale di dati sul traffico e sull'ubicazione di persone determinate, che, pur incidendo sui diritti e sugli obblighi dei fornitori di un servizio di comunicazioni elettroniche, non per questo impone loro uno specifico obbligo di conservazione dei loro dati.

3) Se la direttiva del 12 luglio 2002, letta alla luce della Carta dei diritti fondamentali dell'Unione europea, debba essere interpretata nel senso che essa subordina sempre la regolarità delle procedure di raccolta dei dati di connessione a un obbligo di informazione degli interessati ove tale informazione non sia suscettibile di compromettere le indagini condotte dalle autorità competenti o se tali procedure possano essere considerate regolari, tenuto conto di tutte le altre garanzie procedurali esistenti, una volta che queste ultime garantiscono l'efficacia del diritto di ricorso. **[Or. 15]**

Articolo 3: (omissis) **[Or. 16]**

(omissis)