Raccolta della giurisprudenza

CONCLUSIONI DELL'AVVOCATO GENERALE
MANUEL CAMPOS SÁNCHEZ-BORDONA
presentate il 15 gennaio 2020[1]

Cause riunite C 511/18 e C-512/18

La Quadrature du Net,
French Data Network,
Fédération des fournisseurs d'accès à Internet associatifs,
Igwan.net (C-511/18)
contro
Premier ministre,
Garde des Sceaux, ministre de la Justice,
Ministre de l'Intérieur,
Ministre des Armées

[domanda di pronuncia pregiudiziale proposta dal Conseil d'État (Consiglio di Stato, Francia)]

«Rinvio pregiudiziale – Trattamento di dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche – Salvaguardia della sicurezza nazionale e lotta contro il terrorismo – Direttiva 2002/58/CE – Ambito di applicazione – Articolo 1, paragrafo 3 – Articolo 15, paragrafo 3 – Articolo 4, paragrafo 2, TUE – Carta dei diritti fondamentali dell'Unione europea – Articoli 6, 7, 8, 11, 47 e 52, paragrafo 1 – Conservazione generalizzata e indifferenziata dei dati di connessione e dei dati che consentono di identificare gli autori di contenuti – Raccolta di dati relativi al traffico e all'ubicazione – Accesso ai dati»

1. Negli ultimi anni la Corte ha mantenuto un orientamento giurisprudenziale costante in materia di conservazione e accesso ai dati personali, di cui sono pietre miliari:

– la sentenza dell'8 aprile 2014, Digital Rights Ireland e a.[2], nella quale essa ha dichiarato l'invalidità della direttiva 2006/24/CE[3] in quanto consentiva un'ingerenza non proporzionata nei diritti sanciti dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»);

– la sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a.[4], nella quale ha interpretato l'articolo 15, paragrafo 1, della direttiva 2002/58/CE[5];

1 Lingua originale: lo spagnolo.

2 C-293/12 e C-594/12; in prosieguo: la «sentenza Digital Rights», EU:C:2014:238.

3 Direttiva del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (GU 2006, L 105, pag. 54).

4 C-203/15 e C-698/15, in prosieguo: la «sentenza Tele2 Sverige e Watson», EU:C:2016:970.

5 Direttiva del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU 2002, L 201, pag. 37).

– la sentenza del 2 ottobre 2018, Ministerio Fiscal[6], nella quale ha confermato l'interpretazione della medesima disposizione della direttiva 2002/58.

2. Tali sentenze (in particolare la seconda) suscitano preoccupazione nelle autorità di alcuni Stati membri in quanto, a loro avviso, hanno l'effetto di privarle di uno strumento che esse ritengono imprescindibile per la salvaguardia della sicurezza nazionale e la lotta contro la criminalità e il terrorismo. Alcuni di detti Stati membri chiedono quindi di invertire o temperare la giurisprudenza in parola.

3. Taluni organi giurisdizionali degli Stati membri hanno evidenziato la medesima preoccupazione in quattro rinvii pregiudiziali[7] nei quali presento parimenti in data odierna le mie conclusioni.

4. Le quattro cause sollevano, anzitutto, il problema dell'applicazione della direttiva 2002/58 ad attività inerenti alla sicurezza nazionale e alla lotta contro il terrorismo. Qualora detta direttiva fosse applicabile in tale contesto, occorrerebbe allora chiarire in quale misura gli Stati membri possano limitare il diritto alla vita privata da essa tutelato. Infine, si dovrà esaminare fino a che punto le diverse normative nazionali (quelle del Regno Unito[8], belga[9] e francese[10]) in questa materia siano conformi al diritto dell'Unione, come interpretato dalla Corte.

I. Contesto normativo

A. Diritto dell'Unione

1. Direttiva 2002/58

5. Ai sensi dell'articolo 1 («Finalità e campo d'applicazione»):

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

(…)

3. La presente direttiva non si applica alle attività che esulano dal campo di applicazione del trattato che istituisce la Comunità europea, quali quelle disciplinate dai titoli V e VI del trattato sull'Unione europea né, comunque, alle attività riguardanti la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) o alle attività dello Stato in settori che rientrano nel diritto penale».

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

7 Oltre che delle due presenti (C-511/18 e C-512/18), si tratta delle cause C-623/17, Privacy International, e C-520/18, Ordre des barreaux francophones et germanophone e a.

8 Causa Privacy International, C-623/17.

9 Causa Ordre des barreaux francophones et germanophone e a., C-520/18.

10 Cause La Quadrature du Net e a., C-511/18 e C-512/18.

6. L'articolo 3 («Servizi interessati») così dispone:

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

7. L'articolo 5 («Riservatezza delle comunicazioni»), paragrafo 1, prevede quanto segue:

«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».

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

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

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

9. L'articolo 15 («Applicazione di alcune disposizioni della direttiva 95/46/CE [11]»), paragrafo 1, enuncia quanto segue:

«Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/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».

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

2. Direttiva 2000/31/CE[12]

10. L'articolo 14 stabilisce quanto segue:

«1. Gli Stati membri provvedono affinché, nella prestazione di un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non sia responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore:

(…)

3. Il presente articolo lascia impregiudicata la possibilità, per un organo giurisdizionale o un'autorità amministrativa, in conformità agli ordinamenti giuridici degli Stati membri, di esigere che il prestatore ponga fine ad una violazione o la impedisca nonché la possibilità, per gli Stati membri, di definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime».

11. A termini dell'articolo 15:

«1. Nella prestazione dei servizi di cui agli articoli 12, 13 e 14, 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.

2. Gli Stati membri possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati».

3. Regolamento (UE) 2016/679[13]

12. Ai sensi dell'articolo 2 («Ambito di applicazione materiale»):

«1. Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

2. Il presente regolamento non si applica ai trattamenti di dati personali:

a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;

b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;

c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;

12 Direttiva 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 (direttiva sul commercio elettronico) (GU 2000, L 178, pag. 1).

13 Regolamento 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).

d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

(…)».

13. A tenore dell'articolo 23 («Limitazioni»), paragrafo 1:

«Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare:

a) la sicurezza nazionale;

b) la difesa;

c) la sicurezza pubblica;

d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;

e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;

f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;

g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;

h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a) a e) e g);

i) la tutela dell'interessato o dei diritti e delle libertà altrui;

j) l'esecuzione delle azioni civili».

14. L'articolo 95 («Rapporto con la direttiva 2002/58/CE») così recita:

«Il presente regolamento non impone obblighi supplementari alle persone fisiche o giuridiche in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nell'Unione, per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva 2002/58/CE».

B. Diritto nazionale

1. Code de la sécurité intérieure (codice della sicurezza interna)

15. Ai sensi dell'articolo L. 851-1:

«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 al paragrafo I, punti 1 e 2, dell'articolo 6 della loi n. 2004-575 (…) pour la confiance dans l'économie numérique [(legge n. 2004-575 (…), 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 (…)».

16. Gli articoli L. 851-2 e L. 851-4 disciplinano, per finalità e secondo metodi differenti, gli accessi amministrativi in tempo reale ai dati di connessione così conservati.

17. L'articolo L. 851-2 autorizza, 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 precedentemente identificate come potenzialmente collegate a una minaccia terroristica, è effettuata in tempo reale. Lo stesso vale per l'articolo L. 851-4, che autorizza la trasmissione in tempo reale, da parte degli operatori, dei soli dati tecnici concernenti l'ubicazione delle apparecchiature terminali [14].

18. L'articolo L. 851-3 consente 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» [15].

19. L'articolo L. 851-5 precisa che, a determinate condizioni, «può essere autorizzato l'uso di un dispositivo tecnico che consenta di localizzare in tempo reale persone, veicoli o oggetti».

20. Ai sensi dell'articolo L. 851-6, paragrafo I, è possibile, a determinate condizioni, «raccogliere direttamente, mediante un apparecchio o un dispositivo tecnico di cui all'articolo 226-3, punto 1°, del code pénal [(codice penale)], i dati tecnici di collegamento che consentono di identificare un'apparecchiatura terminale o il numero di abbonamento del relativo utente, nonché i dati relativi all'ubicazione delle apparecchiature terminali utilizzate».

14 Secondo il giudice del rinvio, tali tecniche non pongono a carico dei fornitori di servizi un obbligo di conservazione aggiuntivo rispetto a quanto necessario ai fini della fatturazione e commercializzazione dei loro servizi e della fornitura di servizi a valore aggiunto.

15 Secondo il giudice del rinvio, questa tecnica, che non implica una conservazione generalizzata e indifferenziata, 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.

2. Codice delle poste e delle comunicazioni elettroniche

21. Ai sensi dell'articolo L. 34-1, nella versione applicabile ai fatti:

«I. Il presente articolo si applica al trattamento dei dati personali nella prestazione al pubblico di servizi di comunicazione elettronica; in particolare, si applica alle reti che supportano i dispositivi di raccolta e di identificazione dei dati.

II. Gli operatori di comunicazione elettronica, e in particolare le persone la cui attività consiste nell'offrire accesso a servizi di comunicazione al pubblico online, eliminano o rendono anonimi tutti i dati relativi al traffico, fatte salve le disposizioni dei paragrafi III, IV, V e VI.

Le persone che forniscono al pubblico servizi di comunicazione elettronica stabiliscono, nel rispetto delle disposizioni del comma precedente, procedure interne che consentano di soddisfare le richieste delle autorità competenti.

Le persone che, nell'esercizio di un'attività professionale principale o accessoria, offrono al pubblico una connessione che consente la comunicazione online tramite accesso alla rete, anche a titolo gratuito, sono tenuti al rispetto delle disposizioni applicabili agli operatori di comunicazione elettronica ai sensi del presente articolo.

III. Ai fini dell'indagine, dell'accertamento e del perseguimento dei reati o dell'inadempimento dell'obbligo definito all'articolo L. 336-3 del code de la propriété intellectuelle [(codice della proprietà intellettuale)] o ai fini della prevenzione di attacchi ai sistemi di trattamento automatizzato dei dati previsti e puniti dagli articoli da 323-1 a 323-3-1 del codice penale, e al solo scopo di consentire, ove necessario, la messa a disposizione dell'autorità giudiziaria o dell'alta autorità di cui all'articolo L. 331-12 del codice della proprietà intellettuale o dell'autorità nazionale per la sicurezza dei sistemi di informazione menzionata all'articolo L. 2321-1 del code de la défense [(codice della difesa)], possono essere rinviate per un periodo massimo di un anno le operazioni dirette ad eliminare o a rendere anonime determinate categorie di dati tecnici. Con decreto adottato dopo aver consultato il Conseil d'État [(Consiglio di Stato, Francia)], e previo parere della Commission nationale de l'informatique et des libertés [(Commissione nazionale per l'informatica e le libertà, Francia)], sono stabilite, entro i limiti fissati al paragrafo VI, le suddette categorie di dati e la durata della loro conservazione, in funzione dell'attività degli operatori e della natura delle comunicazioni, nonché, se del caso, le modalità di compensazione delle spese identificabili e specifiche delle prestazioni garantite a tale titolo, su richiesta dello Stato, dagli operatori.

(…)

VI. I dati conservati e trattati alle condizioni di cui ai paragrafi III, IV e V riguardano esclusivamente l'identificazione degli utenti dei servizi prestati dagli operatori, le caratteristiche tecniche delle comunicazioni fornite da questi ultimi e l'ubicazione delle apparecchiature terminali.

Essi non possono riguardare in alcun caso il contenuto della corrispondenza intercorsa o delle informazioni consultate, in qualsiasi modo, nell'ambito di tali comunicazioni.

La conservazione e il trattamento dei dati sono effettuati nel rispetto delle disposizioni della loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [(legge n. 78-17 del 6 gennaio 1978, relativa all'informatica, ai file e alle libertà)].

Gli operatori adottano le misure necessarie per impedire l'utilizzo di tali dati a fini diversi da quelli previsti nel presente articolo».

22. Ai sensi dell'articolo R. 10-13, paragrafo I, gli operatori devono conservare, ai fini dell'indagine, dell'accertamento e del perseguimento dei reati, i seguenti dati:

«a) le informazioni che permettono di identificare l'utente;

b) i dati relativi alle apparecchiature terminali di comunicazione utilizzate;

c) le caratteristiche tecniche nonché la data, l'ora e la durata di ogni comunicazione;

d) i dati relativi ai servizi complementari richiesti o utilizzati e i loro fornitori;

e) i dati che consentono di identificare il destinatario o i destinatari della comunicazione».

23. Ai sensi del paragrafo II dello stesso articolo, nel caso delle attività di telefonia, l'operatore deve inoltre conservare i dati che consentono di identificare l'origine e l'ubicazione della comunicazione.

24. Ai sensi del paragrafo III del medesimo articolo, i dati di cui sopra devono essere conservati per un anno, a decorrere dalla data della loro registrazione.

3. Legge n. 2004-575, del 21 giugno 2004, in materia di promozione della fiducia nell'economia digitale

25. L'articolo 6, paragrafo II, primo comma, della legge n. 2004-575 prevede che le persone la cui attività consiste nell'offrire al pubblico un accesso a servizi di comunicazione online e le persone fisiche o giuridiche che garantiscono, anche a titolo gratuito, mediante la messa a disposizione del pubblico tramite servizi di comunicazione al pubblico online, l'archiviazione di segnali, scritti, immagini, suoni o messaggi di qualsiasi natura forniti dai destinatari di detti servizi, «detengono e conservano i dati con modalità tali da permettere l'identificazione di chiunque abbia contribuito alla creazione del contenuto o di uno dei contenuti dei servizi da esse prestati».

26. Il paragrafo II, terzo comma, del medesimo articolo stabilisce che l'autorità giudiziaria può chiedere a dette persone di comunicarle i dati indicati nel primo comma.

27. Il paragrafo II, ultimo comma, dispone che un decreto del Conseil d'État (Consiglio di Stato) «definisce i dati menzionati nel primo comma nonché la durata e le modalità della loro conservazione» [16].

16 La definizione è stata adottata mediante il décret n.° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (decreto n. 2011-219, del 25 febbraio 2011, sulla conservazione dei dati che consentono l'identificazione di chiunque abbia contribuito alla creazione di un contenuto offerto online). Di tale decreto si possono evidenziare: a) l'articolo 1, paragrafo 1, ai sensi del quale le persone che forniscono un accesso a servizi di comunicazione online devono conservare i seguenti dati: l'identificatore della connessione, l'identificatore attribuito all'abbonato, l'identificatore del terminale utilizzato per la connessione, la data nonché l'ora dell'inizio e della fine della connessione e le caratteristiche della linea dell'abbonato; b) ai sensi dell'articolo 1, paragrafo 2, le persone che garantiscono, anche a titolo gratuito, ai fini della messa a disposizione del pubblico tramite servizi di comunicazione al pubblico online, l'archiviazione di segnali, scritti, immagini, suoni o messaggi di qualsiasi natura forniti dai destinatari di detti servizi, devono conservare, per ogni operazione, i seguenti dati: l'identificatore della connessione all'origine della comunicazione, l'identificatore attribuito al contenuto oggetto dell'operazione, i tipi di protocolli utilizzati per la connessione al servizio e per il trasferimento di contenuti, la natura dell'operazione, la data e l'ora dell'operazione, nonché l'identificatore utilizzato dall'autore dell'operazione; e c) infine, l'articolo 3, paragrafo 1, dispone che le persone menzionate nei due punti precedenti devono conservare le seguenti informazioni fornite dall'utente in occasione della conclusione di un contratto o della creazione di un account: nome, cognome o ragione sociale, gli indirizzi postali associati, gli pseudonimi utilizzati, gli indirizzi di posta elettronica o dell'account associati, i numeri di telefono, la password aggiornata e i dati che consentono di verificarla o modificarla.

II. Fatti e questioni pregiudiziali

A. Causa C-511/18

28. La Quadrature du Net, la French Data Network, la Igwan.net e la Fédération des fournisseurs d'accès à Internet associatifs (in prosieguo: le «ricorrenti») hanno chiesto al Conseil d'État (Consiglio di Stato) di annullare vari decreti di attuazione di alcune disposizioni del codice della sicurezza interna [17].

29. Le ricorrenti hanno sostenuto, in sintesi, che i decreti impugnati, nonché le menzionate disposizioni del codice della sicurezza interna, sarebbero contrari ai diritti al rispetto della vita privata, alla protezione dei dati personali e a un ricorso effettivo, garantiti rispettivamente dagli articoli 7, 8 e 47 della Carta.

30. In tale contesto, il Conseil d'État (Consiglio di Stato) sottopone alla Corte le 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 [2002/58/CE] 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 (…) e dalle esigenze di sicurezza nazionale, la cui responsabilità è rimessa, a norma dell'articolo 4 [TUE], unicamente agli Stati membri.

2) Se la direttiva del 12 luglio 2002, letta alla luce della Carta (…), 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 (…), 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».

B. Causa C-512/18

31. Le ricorrenti nella controversia che ha dato luogo alla causa C-511/18, ad eccezione della Igwan.net, hanno inoltre chiesto al Conseil d'État (Consiglio di Stato) di annullare la decisione (tacita) di rigetto della loro domanda di abrogazione dell'articolo R. 10-13 del codice delle poste e delle comunicazioni elettroniche nonché del decreto n. 2011-219 del 25 febbraio 2011.

17 I decreti impugnati erano i seguenti: a) décret n.º 2015-1885 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); b) décret n.º 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en oeuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (decreto n. 2015-1211, del 1º ottobre 2015, relativo al contenzioso in materia di attuazione delle tecniche di informazione soggette ad autorizzazione e di fascicoli concernenti la sicurezza dello Stato); c) décret n.º 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 libre VIII 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), e d) décret n.º 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).

32. Ad avviso di dette ricorrenti, le disposizioni impugnate impongono un obbligo di conservazione dei dati relativi al traffico, all'ubicazione e alla connessione che, per il suo carattere generale, costituisce un pregiudizio sproporzionato ai diritti al rispetto della vita privata e della vita familiare, alla protezione dei dati di carattere personale e alla libertà di espressione, tutelati dagli articoli 7, 8 e 11 della Carta, in violazione dell'articolo 15, paragrafo 1, della direttiva 2002/58.

33. In tale procedimento, il Conseil d'État (Consiglio di Stato) ha sollevato le seguenti questioni pregiudiziali:

«1) Se, tenuto conto in particolare delle salvaguardie e dei controlli che accompagnano poi la raccolta e l'utilizzo dei dati di connessione di cui trattasi, l'obbligo di conservazione generalizzata e indifferenziata, imposto ai fornitori sulla base delle disposizioni autorizzative di cui all'articolo 15, paragrafo 1, della direttiva [2002/58/CE], debba essere considerato come un'ingerenza giustificata dal diritto alla sicurezza garantito dall'articolo 6 della Carta (…) e dalle esigenze di sicurezza nazionale, la cui responsabilità è rimessa, a norma dell'articolo 4 [TUE], unicamente agli Stati membri.

2) Se le disposizioni della direttiva [2000/31/CE], lette alla luce degli articoli 6, 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta (…), debbano essere interpretate nel senso che esse consentono a uno Stato di prevedere una normativa nazionale che imponga alle persone la cui attività consiste nell'offrire al pubblico un accesso a servizi di comunicazione online e alle persone fisiche o giuridiche che garantiscono, anche a titolo gratuito, mediante la messa a disposizione del pubblico tramite servizi di comunicazione al pubblico online, l'archiviazione di segnali, scritti, immagini, suoni o messaggi di qualsiasi natura forniti dai destinatari di detti servizi, di conservare i dati con modalità tali da consentire l'identificazione di chiunque abbia contribuito alla creazione del contenuto o di uno dei contenuti dei servizi da esse prestati al fine di permettere all'autorità giudiziaria, se del caso, di richiederne la comunicazione per ottenere il rispetto delle norme in materia di responsabilità civile o penale».

III. Procedimento dinanzi alla Corte e posizioni delle parti

34. Le domande di pronuncia pregiudiziale sono pervenute presso la cancelleria della Corte il 3 agosto 2018.

35. Hanno presentato osservazioni scritte la Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, la French Data Network, i governi belga, ceco, cipriota, danese, del Regno Unito, estone, francese, irlandese, polacco, spagnolo, svedese, tedesco e ungherese, nonché la Commissione.

36. Il 9 settembre 2019 si è tenuta un'udienza pubblica, comune anche alle cause C-623/17, Privacy International, e C-520/18, Ordre des barreaux francophones et germanophone e a., alla quale hanno partecipato le parti dei quattro procedimenti pregiudiziali, i governi sopra citati e quelli dei Paesi Bassi e norvegese, nonché la Commissione e il Garante europeo della protezione dei dati.

IV. Analisi

37. Le questioni sollevate dal Conseil d'État (Consiglio di Stato) possono essere suddivise in tre gruppi:

– in primo luogo, se sia compatibile con il diritto dell'Unione una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica l'obbligo di conservare in maniera generalizzata e indifferenziata i dati di connessione (prima questione nella causa C-511/18 e nella causa C-512/18) e, in particolare, i dati che consentono di identificare gli autori dei contenuti offerti da tali fornitori (seconda questione nella causa C-512/18);

– in secondo luogo, se la legittimità delle procedure di raccolta dei dati di connessione sia sempre subordinata a un obbligo di informazione degli interessati ove ciò non comprometta le indagini (terza questione nella causa C-511/18);

– in terzo luogo, se la raccolta in tempo reale di dati sul traffico e sull'ubicazione, senza obbligo di conservarli, sia compatibile – e a quali condizioni – con la direttiva 2002/58 (seconda questione nella causa C-511/18).

38. Occorre stabilire, in definitiva, se sia conforme al diritto dell'Unione una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica due tipi di obblighi: a) da un lato, la *raccolta* di taluni dati, ma non la loro conservazione; b) dall'altro, la *conservazione* dei dati di connessione e dei dati che consentono di identificare le persone che hanno creato i contenuti dei servizi prestati da tali fornitori.

39. In via preliminare si dovrà esaminare se, proprio a motivo del contesto [18] nel quale è stata adottata la normativa nazionale (vale a dire, in circostanze nelle quali potrebbe risultare compromessa la sicurezza nazionale), sia applicabile la direttiva 2002/58.

A. Sull'applicabilità della direttiva 2002/58

40. Il giudice del rinvio considera pacifico che la normativa controversa rientri nell'ambito di applicazione della direttiva 2002/58. Ciò risulta, a suo avviso, dalla giurisprudenza elaborata nella sentenza Tele2 Sverige e Watson e confermata nella sentenza Ministerio Fiscal.

41. Viceversa, alcuni dei governi intervenuti nel procedimento affermano che la normativa controversa non ricade in tale ambito. A sostegno della loro tesi, essi richiamano, tra l'altro, la sentenza del 30 maggio 2006, Parlamento/Consiglio e Commissione [19].

42. Concordo con il Conseil d'État (Consiglio di Stato) sul fatto che la sentenza Tele2 Sverige e Watson ha risolto questa parte della discussione, confermando che la direttiva 2002/58 si applica, in linea di principio, quando i fornitori di servizi di comunicazione elettronica sono tenuti per legge a conservare i dati dei loro abbonati e a consentire alle autorità pubbliche di accedervi. Non influisce su tale tesi la circostanza che gli obblighi siano imposti ai fornitori per motivi di sicurezza nazionale.

43. Devo anticipare fin d'ora che, qualora vi fosse una discordanza fra le precedenti pronunce e la sentenza Tele2 Sverige e Watson, quest'ultima dovrebbe essere considerata prevalente, in quanto successiva e avvalorata dalla sentenza Ministerio Fiscal. Ritengo, tuttavia, che non vi sia alcuna discordanza, come tenterò di spiegare.

18 «[U]n contesto caratterizzato da minacce gravi e persistenti alla sicurezza nazionale, e in particolare dal rischio terroristico», come precisato nella prima questione della causa C-511/18.

19 C-317/04 e C-318/04; in prosieguo: la «sentenza Parlamento/Consiglio e Commissione», EU:C:2006:346.

1. Sentenza Parlamento/Consiglio e Commissione

44. Le cause definite con la sentenza Parlamento/Consiglio e Commissione riguardavano:

– l'accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati PNR [Passenger Name Records (dati di identificazione delle pratiche relative ai passeggeri)] da parte dei vettori aerei alle autorità statunitensi [20];

– il livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri trasferiti a dette autorità [21].

45. La Corte ha concluso che il trasferimento di tali dati costituiva un trattamento avente come oggetto la pubblica sicurezza e le attività dello Stato in materia di diritto penale. Ai sensi dell'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46, le due decisioni controverse non rientravano nell'ambito di applicazione della direttiva 95/46.

46. I dati erano inizialmente raccolti dai vettori aerei nell'ambito di un'attività – la vendita di biglietti – ricompresa nella sfera di applicazione del diritto dell'Unione. Tuttavia, il loro trattamento, quale preso in considerazione nella decisione controversa, non è «necessario alla realizzazione di una prestazione di servizi, ma ritenuto necessario per salvaguardare la pubblica sicurezza e a fini repressivi» [22].

47. La Corte ha dunque adottato un approccio teleologico, tenendo conto dello scopo ricercato con il trattamento dei dati: poiché con quest'ultimo si perseguiva la tutela della sicurezza pubblica, si doveva ritenere che esso esulasse dall'ambito di applicazione della direttiva 95/46. Tuttavia, tale scopo non era l'unico criterio determinante [23], cosicché la sentenza ha sottolineato che esso «rientra in un ambito istituito dai poteri pubblici e attinente alla pubblica sicurezza» [24].

48. La sentenza Parlamento/Consiglio e Commissione consente quindi di valutare la differenza tra la clausola di esclusione e le clausole di restrizione o limitazione della direttiva 95/46 (analoghe a quelle della direttiva 2002/58). È vero, tuttavia, che sia l'una che le altre si riferiscono ad obiettivi di interesse generale analoghi, il che determina una certa confusione sulla loro rispettiva portata, come rilevato a suo tempo dall'avvocato generale Bot [25].

20 Decisione 2004/496/CE del Consiglio, del 17 maggio 2004, relativa alla conclusione di un accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche (Passenger Name Record, PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti (GU 2004, L 183, pag. 83, e rettifica in GU 2005, L 255, pag. 168) (C-317/04).

21 Decisione 2004/535/CE della Commissione, del 14 maggio 2004, relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei trasferiti all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti (GU 2004, L 235, pag. 11) (C-318/04).

22 Sentenza Parlamento/Consiglio e Commissione, punto 57. Al punto 58 viene rilevato che «il fatto che i dati (…) sono stati raccolti da operatori privati a fini commerciali e che sono questi ultimi ad organizzarne il trasferimento ad uno Stato terzo» non implica che tale trasferimento non costituisca una delle ipotesi escluse dall'applicazione della direttiva 95/46 elencate all'articolo 3, paragrafo 2, primo trattino, di quest'ultima, in quanto «il trasferimento rientra in un ambito istituito dai poteri pubblici e attinente alla pubblica sicurezza».

23 Ciò sarebbe stato successivamente evidenziato dal compianto avvocato generale Bot nelle conclusioni nella causa Irlanda/Parlamento e Consiglio (C-301/06, EU:C:2008:558). Egli osservava che la sentenza Parlamento/Consiglio e Commissione «non può significare che solo l'esame dello scopo perseguito da un trattamento di dati personali è pertinente per includere o escludere tale trattamento dall'ambito di applicazione del sistema di protezione dei dati istituito dalla direttiva 95/46. Occorre anche verificare nell'ambito di quale tipo di attività viene effettuato il trattamento dei dati. Solo nel caso in cui venga realizzato nell'esercizio di attività proprie degli Stati o delle autorità statali ed estranee ai settori di attività dei singoli tale trattamento è escluso dal sistema comunitario di protezione dei dati personali risultante dalla direttiva 95/46, in applicazione dell'art. 3, n. 2, primo trattino, di tale direttiva» (paragrafo 122).

24 Sentenza Parlamento/Consiglio e Commissione, punto 58. L'Accordo mirava principalmente ad imporre ai vettori aerei che effettuavano servizi di trasporto di passeggeri tra l'Unione e gli Stati Uniti di fornire alle autorità statunitensi un accesso elettronico ai dati PNR di identificazione delle pratiche relative alle schede nominative dei passeggeri contenuti nei loro sistemi automatici di prenotazione/controllo. Esso istituiva quindi una forma di cooperazione internazionale tra l'Unione e gli Stati Uniti ai fini della lotta contro il terrorismo e altri reati gravi, tentando di conciliare tale obiettivo con quello della protezione dei dati personali dei passeggeri. In siffatto contesto, l'obbligo imposto ai vettori aerei non era molto diverso da uno scambio diretto di dati tra autorità pubbliche.

25 Conclusioni dell'avvocato generale Bot nella causa Irlanda/Parlamento e Consiglio (C-301/06, EU:C:2008:558, paragrafo 127).

49. È probabile che tale confusione sia all'origine della tesi degli Stati membri che sostengono l'inapplicabilità della direttiva 2002/58 al presente contesto. A loro avviso, l'interesse della sicurezza nazionale si tutela solo mediante l'esclusione di cui all'articolo 1, paragrafo 3, della direttiva 2002/58. È indubbio, tuttavia, che perseguono il medesimo interesse anche le limitazioni autorizzate dall'articolo 15, paragrafo 1, della menzionata direttiva, tra cui quella relativa alla sicurezza nazionale. Quest'ultima disposizione sarebbe superflua se la direttiva 2002/58 risultasse inapplicabile a fronte di qualsiasi richiamo alla sicurezza nazionale.

2. Sentenza Tele2 Sverige e Watson

50. Nella sentenza Tele2 Sverige e Watson è stata esaminata la compatibilità con il diritto dell'Unione di taluni regimi nazionali che imponevano ai fornitori di servizi di comunicazione elettronica accessibili al pubblico un obbligo generale di conservazione dei dati relativi a dette comunicazioni. Le fattispecie erano quindi sostanzialmente identiche a quella oggetto dei presenti rinvii pregiudiziali.

51. Interpellata nuovamente in merito all'applicabilità del diritto dell'Unione – questa volta già in vigenza della direttiva 2002/58 –, la Corte ha rilevato anzitutto che «l'ampiezza dell'ambito di applicazione della direttiva 2002/58 deve essere valutata tenendo conto in particolare dell'economia generale di quest'ultima» [26].

52. In tale prospettiva, la Corte ha osservato che, «[c]erto, le disposizioni legislative contemplate dall'articolo 15, paragrafo 1, della direttiva 2002/58 si riferiscono ad attività proprie degli Stati o delle autorità statali, estranee ai settori di attività dei singoli (…). Inoltre, le finalità che, in forza del citato articolo 15, paragrafo 1, le disposizioni legislative suddette devono soddisfare – nella fattispecie, la salvaguardia della sicurezza nazionale (…) – coincidono sostanzialmente con le finalità perseguite dalle attività contemplate dall'articolo 1, paragrafo 3, della medesima direttiva» [27].

53. Pertanto, la finalità delle misure che possono essere adottate dagli Stati membri ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58 per limitare il diritto alla vita privata coincide (su questo punto) con quella che giustifica l'esenzione di talune attività statali dal regime della direttiva, conformemente all'articolo 1, paragrafo 3, della stessa.

54. Tuttavia, la Corte ha ritenuto che, «alla luce dell'economia generale della direttiva 2002/58», siffatta circostanza non consentisse di «concludere che le misure legislative contemplate dall'articolo 15, paragrafo 1, della direttiva 2002/58 siano escluse dall'ambito di applicazione di tale direttiva, a pena di privare detta disposizione di qualsiasi effetto utile. Infatti, il citato articolo 15, paragrafo 1, presuppone necessariamente che le misure nazionali da esso contemplate (…) rientrino nell'ambito di applicazione di questa medesima direttiva, dato che quest'ultima autorizza espressamente gli Stati membri ad adottare le misure in questione unicamente a condizione di rispettare le condizioni da essa previste» [28].

55. A quanto precede si aggiunge il fatto che le limitazioni autorizzate dall'articolo 15, paragrafo 1, della direttiva 2002/58 «disciplinano, per le finalità menzionate in tale disposizione, l'attività dei fornitori di servizi di comunicazione elettronica». Ne consegue che detta disposizione, letta in connessione con l'articolo 3 della medesima direttiva, «deve essere interpretat[a] nel senso che siffatte misure legislative rientrano nell'ambito di applicazione della direttiva stessa» [29].

26 Sentenza Tele2 Sverige e Watson, punto 67.

27 Ibidem, punto 72.

28 Ibidem, punto 73.

29 Ibidem, punto 74.

56. Di conseguenza, la Corte ha sostenuto che rientrano nell'ambito di applicazione della direttiva 2002/58 sia una misura legislativa che imponga ai fornitori «di conservare i dati relativi al traffico e i dati relativi all'ubicazione, in quanto una siffatta attività implica necessariamente un trattamento, da parte di tali soggetti, di dati personali» [30], sia una misura legislativa riguardante l'accesso delle autorità ai dati conservati da detti fornitori [31].

57. L'interpretazione della direttiva 2002/58 accolta dalla Corte nella sentenza Tele2 Sverige e Watson è ribadita nella sentenza Ministerio Fiscal.

58. Si può affermare che la sentenza Tele2 Sverige e Watson rappresenta un cambiamento di orientamento, più o meno esplicito, rispetto alla giurisprudenza elaborata nella sentenza Parlamento/Consiglio e Commissione? Ciò è quanto ritiene, ad esempio, il governo irlandese, secondo cui solo quest'ultima sarebbe compatibile con la base giuridica della direttiva 2002/58 e conforme all'articolo 4, paragrafo 2, TUE [32].

59. Il governo francese, dal canto suo, sostiene che la contraddizione può essere evitata ove si consideri che la giurisprudenza della sentenza Tele2 Sverige e Watson riguarda attività degli Stati membri nel settore del diritto penale, mentre quella stabilita nella sentenza Parlamento/Consiglio e Commissione concerne la sicurezza dello Stato e la difesa. Pertanto, la giurisprudenza della sentenza Tele2 Sverige e Watson non sarebbe applicabile al caso in esame, nel quale occorrerebbe attenersi alla soluzione adottata nella sentenza Parlamento/Consiglio e Commissione [33].

60. Come ho già anticipato, credo che si possa trovare una via per integrare le due sentenze, diversa da quella proposta dal governo francese. Non condivido quest'ultima, in quanto, a mio avviso, le considerazioni della sentenza Tele2 Sverige e Watson espressamente riferite alla lotta contro il terrorismo [34] possono essere estese a qualsiasi minaccia contro la sicurezza nazionale (essendo il terrorismo solo una tra altre).

3. Possibilità di un'interpretazione che integri la sentenza Parlamento/Consiglio e Commissione con la sentenza Tele2 Sverige e Watson

61. A mio avviso, nelle sentenze Tele2 Sverige e Watson e Ministerio Fiscal, la Corte ha tenuto conto della ratio delle clausole di esclusione e di restrizione nonché del rapporto sistematico tra i due tipi di clausole.

62. Se nella causa Parlamento/Consiglio e Commissione la Corte ha dichiarato che il trattamento dei dati esulava dall'ambito della direttiva 95/46, ciò era dovuto, come ho già ricordato, alla circostanza che, nel contesto della cooperazione tra l'Unione europea e gli Stati Uniti, in un ambito tipicamente internazionale, la dimensione statale dell'attività doveva prevalere sul fatto che tale trattamento presentava anche una dimensione commerciale o privata. Una delle questioni discusse in quell'occasione era per l'appunto la base giuridica appropriata per la decisione controversa.

63. Al contrario, per quanto riguarda le misure nazionali esaminate nelle sentenze Tele2 Sverige e Watson e Ministerio Fiscal, la Corte ha posto in primo piano la portata interna del trattamento dei dati: il contesto normativo nel quale esso aveva luogo era esclusivamente nazionale ed era quindi assente la dimensione esterna che caratterizzava l'oggetto della sentenza Parlamento/Consiglio e Commissione.

30 Ibidem, punto 75.

31 Ibidem, punto 76.

32 Punti 15 e 16 delle osservazioni scritte del governo irlandese.

33 Punti da 34 a 50 delle osservazioni scritte del governo francese.

34 Sentenza Tele2 Sverige e Watson, punti 103 e 119.

64. La diversa importanza delle dimensioni internazionale e interna (commerciale e privata) del trattamento dei dati ha comportato che, nel primo caso, la clausola di esclusione del diritto dell'Unione sia stata imposta in quanto più adeguata per la tutela dell'interesse generale rappresentato dalla sicurezza nazionale. Nel secondo, viceversa, questo medesimo interesse poteva essere efficacemente soddisfatto mediante la clausola di limitazione prevista all'articolo 15, paragrafo 1, della direttiva 2002/58.

65. Si potrebbe ancora rilevare un'altra differenza, legata al diverso contesto normativo: le due sentenze in parola sono incentrate sull'interpretazione di due disposizioni che, al di là delle apparenze, non sono uguali.

66. Così, la sentenza Parlamento/Consiglio e Commissione ha statuito sull'interpretazione dell'articolo 3, paragrafo 2, della direttiva 95/46, mentre la sentenza Tele2 Sverige e Watson lo ha fatto in relazione all'articolo 1, paragrafo 3, della direttiva 2002/58. La lettura attenta di tali disposizioni evidenzia una differenza sufficiente per confermare il senso delle pronunce della Corte nell'uno e nell'altro caso.

67. Ai sensi dell'articolo 3, paragrafo 2, della direttiva 95/46, «[l]e disposizioni della presente direttiva *non si applicano ai trattamenti di dati personali* (…) effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario (…) e comunque ai *trattamenti* aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali *trattamenti* siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale» [35].

68. D'altro canto, conformemente all'articolo 1, paragrafo 3, della direttiva 2002/58, quest'ultima «*non si applica alle attività* che esulano dal campo di applicazione del trattato che istituisce la Comunità europea (…) 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» [36].

69. Mentre l'articolo 3, paragrafo 2, della direttiva 95/46 esclude i *trattamenti* aventi come oggetto – per quanto qui rileva – la sicurezza dello Stato, l'articolo 1, paragrafo 3, della direttiva 2002/58 esclude le *attività* dirette a tutelare – sempre per quanto qui rileva – la sicurezza dello Stato.

70. La differenza non è di poco conto. La direttiva 95/46 lasciava fuori dal proprio ambito di applicazione un'attività (il «trattamento di dati personali») che può svolgere chiunque. Da tale attività erano specificamente esclusi i trattamenti aventi per oggetto, tra l'altro, la sicurezza dello Stato. Era invece irrilevante la natura del *soggetto* che effettuava il trattamento dei dati. L'approccio adottato per individuare le azioni escluse era quindi teleologico o finalistico, senza distinzione tra le persone che le compievano.

71. Si comprende quindi perché, nella causa Parlamento/Consiglio e Commissione, la Corte abbia preso in considerazione principalmente la finalità perseguita con il trattamento dei dati. A nulla rilevava «il fatto che i dati (…) sono stati raccolti da operatori privati a fini commerciali e che sono questi ultimi ad organizzarne il trasferimento ad uno Stato terzo», in quanto l'elemento determinante era che «il trasferimento rientra in un ambito istituito dai poteri pubblici e attinente alla pubblica sicurezza» [37].

35 Il corsivo è mio.

36 Il corsivo è mio.

37 Sentenza Parlamento/Consiglio e Commissione, punto 58.

72. Per contro, «le attività riguardanti la sicurezza dello Stato», che esulano dall'ambito di applicazione della direttiva 2002/58 esaminato nella causa Tele2 Sverige e Watson, non possono essere svolte da chiunque, bensì unicamente dallo Stato stesso. Inoltre, non rientrano fra tali attività le funzioni normative o di regolamentazione dello Stato, ma strettamente le azioni materiali dei poteri pubblici.

73. Infatti, le *attività* elencate all'articolo 1, paragrafo 3, della direttiva 2002/58 «sono, in tutti i casi, attività proprie degli Stati o delle autorità statali, estranee ai settori di attività dei singoli» [38]. Orbene, tali «attività» non possono avere natura normativa. Se così fosse, tutte le disposizioni adottate dagli Stati membri in relazione al trattamento di dati personali sarebbero escluse dall'ambito di applicazione della direttiva 2002/58, purché si affermi che sono giustificate in quanto necessarie per garantire la sicurezza dello Stato.

74. Da un lato, ciò comporterebbe una notevole perdita di efficacia di detta direttiva, in quanto la mera invocazione di un concetto giuridico così indeterminato come quello della sicurezza nazionale sarebbe sufficiente per rendere inapplicabili nei confronti degli Stati membri le tutele ideate dal legislatore dell'Unione per proteggere i dati personali dei cittadini. Tale protezione è impraticabile senza il concorso degli Stati membri ed è garantita ai cittadini anche nei confronti dei poteri pubblici nazionali.

75. Dall'altro, un'interpretazione della nozione di «attività statali» che comprendesse quelle che si traducono nell'adozione di normative e disposizioni giuridiche svuoterebbe di significato l'articolo 15 della direttiva 2002/58, che autorizza per l'appunto gli Stati membri – per motivi di tutela, inter alia, della sicurezza nazionale – ad adottare «disposizioni legislative» al fine di limitare la portata di taluni diritti ed obblighi previsti dalla medesima direttiva [39].

76. Come ha sottolineato la Corte nella causa Tele2 Sverige e Watson, «l'ampiezza dell'ambito di applicazione della direttiva 2002/58 deve essere valutata tenendo conto in particolare dell'economia generale di quest'ultima» [40]. In tale prospettiva, l'interpretazione dell'articolo 1, paragrafo 3, e dell'articolo 15, paragrafo 1, della direttiva 2002/58 che li dota di significato senza intaccare la loro efficacia è quella che individua, nella prima delle due disposizioni, un'esclusione materiale relativa alle *attività* svolte dagli Stati membri nell'ambito della sicurezza nazionale (o equivalenti) e, nella seconda, un'autorizzazione ad adottare *disposizioni legislative* (vale a dire, norme di applicazione generale) che, per motivi di sicurezza nazionale, incidono sulle attività degli individui soggetti all'imperium degli Stati membri, limitando i diritti garantiti dalla direttiva 2002/58.

38 Sentenza Ministerio Fiscal, punto 32. Nello stesso senso, sentenza Tele2 Sverige e Watson, punto 72.

39 Sarebbe difficile, infatti, sostenere che l'articolo 15, paragrafo 1, della direttiva 2002/58 consente di limitare i diritti e gli obblighi da essa sanciti in un ambito che, come quello della sicurezza nazionale, esulerebbe, in linea di principio, dal suo ambito di applicazione, ai sensi dell'articolo 1, paragrafo 3, della medesima direttiva. Come dichiarato dalla Corte nella sentenza Tele2 Sverige e Watson, punto 73, l'articolo 15, paragrafo 1, della direttiva 2002/58 «presuppone necessariamente che le misure nazionali da esso contemplate (…) rientrino nell'ambito di applicazione di questa medesima direttiva, dato che quest'ultima autorizza espressamente gli Stati membri ad adottare le misure in questione unicamente a condizione di rispettare le condizioni da essa previste».

40 Sentenza Tele2 Sverige e Watson, punto 67.

4. Esclusione della sicurezza nazionale nella direttiva 2002/58

77. La sicurezza nazionale (o l'espressione equivalente «la sicurezza dello Stato», come indicato al suo articolo 15, paragrafo 1) è oggetto di una duplice presa in considerazione nella direttiva 2002/58. Da un lato, essa costituisce un motivo di *esclusione* (dell'applicazione di tale direttiva) per tutte quelle attività degli Stati membri che la «riguard[ano]» specificamente. Dall'altro, si presenta come un motivo di *limitazione*, che deve essere attuato in sede legislativa, dei diritti e degli obblighi stabiliti dalla direttiva 2002/58, vale a dire, in relazione ad attività di natura privata o commerciale ed estranee al settore delle attività sovrane [41].

78. A quali attività si riferisce l'articolo 1, paragrafo 3, della direttiva 2002/58? A mio avviso, lo stesso Conseil d'État (Consiglio di Stato) ne fornisce un valido esempio quando menziona gli articoli L. 851-5 e L. 851-6 del codice della sicurezza interna, in riferimento alle «tecniche di raccolta di informazioni che sono attuate direttamente dallo Stato, ma che non disciplinano le attività dei fornitori di servizi di comunicazione elettronica imponendo loro obblighi specifici» [42].

79. Ritengo che risieda qui la chiave per comprendere l'ambito di esclusione dell'articolo 1, paragrafo 3, della direttiva 2002/58. Non sono soggette al suo regime le *attività* che, essendo dirette a salvaguardare la sicurezza nazionale, vengono svolte autonomamente dai poteri pubblici, senza che sia necessaria la collaborazione di soggetti privati e, pertanto, senza imporre a questi ultimi obblighi riguardanti la gestione delle loro imprese.

80. Tuttavia, l'elenco delle attività delle autorità pubbliche escluse dal regime generale relativo al trattamento dei dati personali deve essere interpretato restrittivamente. In pratica, la nozione di sicurezza nazionale, sulla quale ogni Stato membro ha competenza esclusiva ai sensi dell'articolo 4, paragrafo 2, TUE, non può essere estesa ad altri settori, più o meno correlati, della vita pubblica.

81. Poiché nei presenti procedimenti pregiudiziali sono coinvolti dei privati (vale a dire, soggetti che prestano agli utenti i servizi di comunicazione elettronica) e non vi è solo l'intervento delle autorità statali, non sarà necessario soffermarsi ulteriormente sulla delimitazione dei contorni della sicurezza nazionale stricto sensu.

82. Ritengo, tuttavia, che possa servire come orientamento il criterio della decisione quadro 2006/960/GAI [43], il cui articolo 2, lettera a), distingue tra autorità incaricate dell'applicazione della legge in senso ampio – che comprendono «la polizia, i servizi doganali o altra autorità nazionale che, in forza della legislazione interna, è competente a individuare, prevenire e indagare su reati o attività criminali, esercitare l'autorità e adottare misure coercitive nell'ambito di tali funzioni» –, da un lato, e i «servizi o le unità che si occupano specificamente di questioni connesse alla sicurezza nazionale», dall'altro [44].

41 Come rilevava, incidentalmente, l'avvocato generale Saugmandsgaard Øe nelle conclusioni nella causa Ministerio Fiscal (C-207/16, EU:C:2018:300, paragrafo 47), «non si devono confondere, da una parte, i dati personali trattati *direttamente* nell'ambito delle attività – di natura sovrana – dello Stato in un settore rientrante nel diritto penale e, dall'altra, quelli trattati nell'ambito delle attività – di natura commerciale – di un fornitore di servizi di comunicazione elettronica che sono *successivamente* utilizzati dalle autorità statali competenti».

42 Punti 18 e 21 della decisione di rinvio nella causa C-511/18.

43 Decisione quadro del Consiglio, del 18 dicembre 2016, relativa alla semplificazione dello scambio di informazioni e intelligence tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge (GU 2006, L 386, pag. 89).

44 Nel medesimo senso, l'articolo 1, paragrafo 4, della decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (GU 2008, L 350, pag. 60), prevedeva che essa «lascia[va] impregiudicati gli interessi fondamentali della sicurezza nazionale e specifiche attività di informazione nel settore della sicurezza nazionale».

83. Il considerando 11 della direttiva 2002/58 enuncia che essa, «analogamente alla direttiva 95/46(…), non affronta le questioni relative alla tutela dei diritti e delle libertà fondamentali inerenti ad attività che non sono disciplinate dal diritto [dell'Unione]». Pertanto, la direttiva 2002/58 «[l]ascia (…) 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, [di detta] direttiva, necessari per tutelare (…) la sicurezza dello Stato (…)».

84. Esiste, infatti, una continuità tra la direttiva 95/46 e la direttiva 2002/58 per quanto riguarda le competenze degli Stati membri in materia di sicurezza nazionale. Nessuna delle due ha per oggetto la tutela dei diritti fondamentali in tale specifico settore, nel quale le attività degli Stati membri non sono «disciplinate dal diritto [dell'Unione]».

85. L'«equilibrio» al quale fa riferimento il succitato considerando deriva dalla necessità di rispettare le competenze degli Stati membri in materia di sicurezza nazionale, allorché essi le esercitino *in modo diretto e con i propri mezzi*. Viceversa, allorché, anche per questi stessi motivi di sicurezza nazionale, sia richiesta la collaborazione di privati, ai quali vengono imposti determinati obblighi, tale circostanza comporta l'ingresso in un ambito (la tutela della vita privata richiesta a detti operatori privati) disciplinato dal diritto dell'Unione.

86. Sia la direttiva 95/46 che la direttiva 2002/58 mirano a raggiungere il menzionato equilibrio consentendo che i diritti dei privati siano limitati in forza di misure legislative adottate dagli Stati ai sensi rispettivamente dei loro articoli 13, paragrafo 1, e 15, paragrafo 1. Su questo punto non vi è alcuna differenza tra l'una e l'altra.

87. Quanto al regolamento 2016/679, che definisce un (nuovo) quadro generale per la protezione dei dati personali, il suo articolo 2, paragrafo 2, esclude i «trattamenti di dati personali» effettuati dagli Stati membri «nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE».

88. Mentre nella direttiva 95/46 il trattamento di dati personali era qualificato solo dalla sua finalità, a prescindere dal soggetto che lo effettuava, nel regolamento 2016/679 i trattamenti esclusi sono identificati in funzione sia della loro finalità, sia dei loro autori: si eccettuano quelli realizzati dagli Stati membri nell'esercizio di un'*attività* non compresa nell'ambito di applicazione del diritto dell'Unione [articolo 2, paragrafo 2, lettere a) e b)], e quelli effettuati dalle autorità *ai fini della lotta contro i reati e della protezione* contro le minacce alla sicurezza pubblica [45].

89. La definizione di tali attività delle autorità pubbliche deve essere necessariamente restrittiva, per non privare di qualsiasi efficacia la normativa dell'Unione in materia di tutela della vita privata. Il regolamento 2016/679 contempla all'articolo 23 – sulla scia dell'articolo 15, paragrafo 1, della direttiva 2002/58 – la limitazione, *mediante misure legislative*, dei diritti e degli obblighi da esso previsti, quando sia necessaria per salvaguardare, tra l'altro, la sicurezza nazionale, la difesa o la sicurezza pubblica. Ancora una volta, se la tutela di tali obiettivi fosse sufficiente a determinare l'esclusione dall'ambito di applicazione del regolamento 2016/679, sarebbe superfluo invocare la sicurezza nazionale per giustificare la restrizione, mediante misure legislative, dei diritti garantiti da detto regolamento.

45 Il regolamento 2016/679 esclude, infatti, i trattamenti di dati effettuati dagli Stati membri nell'esercizio di un'*attività* che non rientra nell'ambito di applicazione del diritto dell'Unione, oltre a quelli eseguiti dalle autorità *ai fini della tutela* della sicurezza pubblica.

90. Come nel caso della direttiva 2002/58, non sarebbe coerente che le misure legislative di cui all'articolo 23 del regolamento 2016/679 (che, ripeto, autorizza le limitazioni nazionali al diritto alla vita privata dei cittadini per motivi di sicurezza dello Stato) rientrassero nell'ambito di applicazione di quest'ultimo e, al contempo, la copertura della sicurezza dello Stato rendesse inapplicabile, sic et simpliciter, il medesimo regolamento, con conseguente assenza di riconoscimento di qualsiasi diritto soggettivo.

B. Conferma e possibilità di sviluppo della giurisprudenza Tele2 Sverige e Watson

91. Nelle mie conclusioni nella causa C-520/18 svolgo un esame dettagliato [46] della giurisprudenza della Corte in tale materia, in esito al quale propongo di confermarla, suggerendo al contempo alcune vie interpretative per affinarne il contenuto.

92. Rinvio a tale analisi, che non ritengo necessario trascrivere qui per mera economia. Le considerazioni che svolgerò nel prosieguo sulle questioni pregiudiziali sollevate dal Conseil d'État (Consiglio di Stato) vanno quindi lette assumendo come presupposto le parti corrispondenti delle conclusioni nella causa C-520/18.

C. Risposta alle questioni pregiudiziali

1. Sull'obbligo di conservazione dei dati (prima questione pregiudiziale nelle cause C-511/18 e C-512/18 e seconda questione pregiudiziale nella causa C-512/18)

93. Per quanto riguarda l'obbligo di conservazione dei dati imposto ai fornitori di servizi di comunicazione elettronica, il giudice del rinvio chiede, in concreto:

– se tale obbligo, di cui può esigersi il rispetto in forza dell'articolo 15, paragrafo 1, della direttiva 2002/58, costituisca un'ingerenza giustificata dal «diritto alla sicurezza» garantito dall'articolo 6 della Carta e da imperativi di sicurezza nazionale (prima questione nelle cause C-511/18 e C-512/18 nonché terza questione nella causa C-511/18).

– se la direttiva 2000/31 consenta la conservazione di dati che possono permettere di identificare chiunque abbia contribuito alla creazione dei contenuti accessibili al pubblico online (seconda questione nella causa C-512/18).

a) Osservazioni preliminari

94. Il Conseil d'État (Consiglio di Stato) fa riferimento ai diritti fondamentali riconosciuti agli articoli 7 (rispetto della vita privata e della vita familiare), 8 (protezione dei dati di carattere personale) e 11 (libertà di espressione e d'informazione) della Carta. Sono questi, in effetti, i diritti che, secondo la Corte, potrebbero essere lesi dall'obbligo di conservazione dei dati relativi al traffico imposto dalle autorità nazionali ai fornitori di servizi di comunicazione elettronica [47].

95. Il giudice del rinvio fa inoltre riferimento al diritto alla sicurezza tutelato dall'articolo 6 della Carta. Più che come diritto eventualmente leso, esso lo evoca in quanto fattore che potrebbe legittimare l'imposizione del suddetto obbligo.

46 Paragrafi da 27 a 68.

47 V., in tal senso, sentenza Tele2 Sverige e Watson, punto 92, che richiama, per analogia, la sentenza Digital Rights, punti 25 e 70.

96. Concordo con la Commissione sul fatto che il richiamo in questi termini all'articolo 6 può risultare fuorviante. Al pari della Commissione, ritengo che la disposizione non debba essere interpretata nel senso che è idonea «ad imporre all'Unione un obbligo positivo di adottare misure dirette a proteggere le persone da atti criminosi» [48].

97. La sicurezza garantita dal succitato articolo della Carta non si identifica con la sicurezza pubblica. O, se si preferisce, essa riguarda tanto quest'ultima quanto qualsiasi altro diritto fondamentale, in quanto la sicurezza pubblica è una condizione indispensabile per il godimento dei diritti e delle libertà fondamentali.

98. Come ricordato dalla Commissione, l'articolo 6 della Carta, secondo quanto affermato nelle spiegazioni che l'accompagnano, corrisponde all'articolo 5 della Convenzione europea dei diritti dell'uomo (in prosieguo: la «CEDU»). Dalla lettura dell'articolo 5 della CEDU emerge che la «sicurezza» ivi tutelata è strettamente la sicurezza personale, intesa come garanzia del diritto alla libertà fisica dall'arresto o dalla detenzione arbitrari. La sicurezza, in definitiva, che nessuno può essere privato della libertà, salvo nei casi, alle condizioni e secondo le procedure previste dalla legge.

99. Si tratta pertanto della *sicurezza personale*, riferita alle condizioni nelle quali può essere limitata la libertà fisica delle persone [49], e non della *sicurezza pubblica* inerente all'esistenza dello Stato, che costituisce il presupposto imprescindibile, in una società sviluppata, per conciliare l'esercizio dei poteri pubblici con il godimento dei diritti individuali.

100. Alcuni governi, tuttavia, chiedono che sia tenuto in maggiore considerazione il diritto alla sicurezza nel secondo di tali significati. Invero, la Corte non lo ha ignorato, anzi, lo ha espressamente menzionato nelle sue sentenze [50] e nei suoi pareri [51]. Essa non ha mai negato l'importanza degli obiettivi di interesse generale della tutela della sicurezza nazionale e dell'ordine pubblico [52], della lotta contro il terrorismo internazionale per il mantenimento della pace e della sicurezza internazionali nonché della lotta contro i reati gravi al fine di garantire la sicurezza pubblica [53], che ha definito, giustamente, «di capitale importanza» [54]. Come ha rilevato a suo tempo, «la protezione della sicurezza pubblica contribuisce altresì alla tutela dei diritti e delle libertà altrui» [55].

101. Si potrebbe approfittare dell'opportunità offerta dai presenti rinvii pregiudiziali per proporre più chiaramente la ricerca di un equilibrio tra, da un lato, il diritto alla sicurezza e, dall'altro, il diritto alla vita privata e il diritto alla protezione dei dati personali. In tal modo si eviterebbero le critiche secondo le quali si favoriscono i secondi a scapito del primo.

102. A tale equilibrio si riferiscono, a mio parere, il considerando 11 e l'articolo 15, paragrafo 1, della direttiva 2002/58, laddove menzionano i requisiti di necessità e proporzionalità delle misure *in una società democratica*. Il diritto alla sicurezza, ripeto, è consustanziale alla stessa esistenza e sopravvivenza di una democrazia, il che giustifica il fatto che se ne tenga pienamente conto nell'ambito della valutazione di detta proporzionalità. In altri termini, se pure la tutela del principio della riservatezza dei dati è fondamentale in una società democratica, tuttavia non si deve sottovalutare l'importanza della sicurezza di quest'ultima.

48 Punto 37 delle osservazioni scritte della Commissione.

49 È questa l'interpretazione accolta dalla Corte EDU.V., per tutte, sentenza del 5 luglio 2016, Buzadji c. Repubblica di Moldova, ECHR:2016:0705JUD002375507, al cui § 84 si afferma che lo scopo fondamentale del diritto sancito dall'articolo 5 della CEDU è prevenire la privazione arbitraria o ingiustificata della libertà individuale.

50 Sentenza Digital Rights, punto 42.

51 Parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017 (in prosieguo: il «parere 1/15», EU:C:2017:592, punto 149 e giurisprudenza citata).

52 Sentenza del 15 febbraio 2016, N. (C-601/15 PPU, EU:C:2016:84, punto 53).

53 Sentenza Digital Rights, punto 42 e giurisprudenza citata.

54 Ibidem, punto 51.

55 Parere 1/15, punto 149.

103. Il contesto segnato dalle minacce gravi e persistenti alla sicurezza nazionale e, in particolare, dal rischio di terrorismo, deve quindi essere preso in considerazione, in linea con quanto dichiarato nell'ultima frase del punto 119 della sentenza Tele2 Sverige e Watson. Un sistema nazionale può reagire in modo proporzionato alla natura e all'intensità delle minacce cui è confrontato senza che tale reazione debba essere necessariamente identica a quella di altri Stati membri.

104. Devo aggiungere, infine, che le suesposte considerazioni non ostano a che, in situazioni propriamente *eccezionali*, caratterizzate da una minaccia imminente o da un rischio di natura straordinaria tali da giustificare la dichiarazione ufficiale dello stato di emergenza in uno Stato membro, la legislazione nazionale preveda, per un periodo limitato, la possibilità di imporre un obbligo di conservazione dei dati tanto ampio e generale quanto si ritenga necessario [56].

105. Di conseguenza, occorrerebbe riformulare la prima questione di entrambi i rinvii pregiudiziali, orientandola piuttosto verso la possibilità di giustificare l'ingerenza con motivi di sicurezza nazionale. Si dovrebbe quindi stabilire se l'obbligo imposto agli operatori di servizi di comunicazione elettronica sia compatibile con l'articolo 15, paragrafo 1, della direttiva 2002/58.

b) Valutazione

1) Caratterizzazione delle norme interne, quali indicate nei due rinvii pregiudiziali, alla luce della giurisprudenza della Corte di giustizia

106. Secondo le decisioni di rinvio, la normativa controversa nei procedimenti principali impone di conservare i dati:

– agli operatori di comunicazione elettronica e, in particolare, a chiunque offra accesso a servizi di comunicazione al pubblico online; e

– alle persone fisiche o giuridiche che garantiscono, anche a titolo gratuito, mediante la messa a disposizione del pubblico online, l'archiviazione di segnali, scritti, suoni, immagini o messaggi di qualsiasi natura forniti dai destinatari di detti servizi [57].

107. Gli operatori devono conservare, per un anno a decorrere dalla data della loro registrazione, le informazioni che consentono di identificare l'utente, i dati relativi alle apparecchiature terminali di comunicazione utilizzate, le caratteristiche tecniche, la data, l'ora e la durata di ogni chiamata, i dati relativi ai servizi complementari richiesti o utilizzati e i loro fornitori, nonché i dati che consentono di identificare il destinatario della comunicazione e, nel caso delle attività di telefonia, l'origine e l'ubicazione della comunicazione [58].

108. Per quanto riguarda, in particolare, i servizi di accesso a internet e i servizi di memorizzazione, sembra che la normativa nazionale richieda la conservazione degli indirizzi IP [59], dei codici di accesso e, qualora sia stato sottoscritto un contratto o un account di pagamento, il tipo di pagamento effettuato, nonché il suo numero di riferimento, l'importo, la data e l'ora dell'operazione [60].

56 V. paragrafi da 105 a 107 delle mie conclusioni nella causa C-520/18.

57 Ciò risulta dall'articolo L. 851-1 del codice della sicurezza interna, che rinvia all'articolo L. 34-1 del codice delle poste e delle comunicazioni elettroniche e all'articolo 6 della legge n. 2004-575, in materia di promozione della fiducia nell'economia digitale.

58 Così dispone l'articolo R. 10-13 del codice delle poste e delle comunicazioni elettroniche.

59 Spetta al giudice del rinvio verificare tale circostanza, sulla quale sono state fornite indicazioni contrastanti in udienza.

60 Articolo 1 del decreto n. 2011-219.

109. Tale obbligo di conservazione è imposto ai fini della ricerca, dell'accertamento e del perseguimento dei reati [61]. In altri termini, a differenza – come si vedrà – di quanto accade con l'obbligo di *raccogliere* dati relativi al traffico e all'ubicazione, l'obbligo di *conservarli* non ha quale unico obiettivo la prevenzione del terrorismo [62].

110. Quanto alle condizioni di *accesso* ai dati conservati, dalle informazioni fornite nel fascicolo emerge che o si tratta di quelle previste dal regime comune (intervento dell'autorità giudiziaria), oppure tale accesso è riservato ad agenti individualmente designati e abilitati, previa autorizzazione del Primo ministro emessa sulla base del parere non vincolante di un'autorità amministrativa indipendente [63].

111. Si comprende facilmente che, come rilevato dalla Commissione [64], i dati di cui le norme nazionali richiedono la conservazione corrispondono, in sostanza, a quelli esaminati dalla Corte nelle sentenze Digital Rights e Tele2 Sverige e Watson [65]. Al pari di quanto accadeva in quei casi, tali dati sono oggetto di un «obbligo di conservazione generalizzata e indifferenziata», come osservato, con franchezza, dal Conseil d'État (Consiglio di Stato) all'inizio delle sue questioni pregiudiziali.

112. Se è così, circostanza questa la cui verifica spetta in definitiva al giudice del rinvio, si deve concludere che la normativa di cui trattasi comporta un'«ingerenza (…) nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta [che] risulta essere di vasta portata e deve essere considerata particolarmente grave» [66].

113. Nessuna delle parti intervenute nei procedimenti ha messo in dubbio che una normativa con siffatte caratteristiche comporti un'ingerenza in tali diritti. Non occorre soffermarsi ora su questo punto, neppure per ricordare che la lesione di detti diritti pregiudica inevitabilmente i fondamenti stessi di una società che mira a rispettare, tra altri valori, la vita privata tutelata dalla Carta.

114. L'applicazione della dottrina elaborata nella sentenza Tele2 Sverige e Watson e confermata dalla sentenza Ministerio Fiscal indurrebbe automaticamente a sostenere che una normativa come quella controversa «travalica (…) i limiti dello stretto necessario e non può essere considerata giustificata, in una società democratica, così come richiede 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» [67].

115. Infatti, al pari di quella esaminata nella sentenza Tele2 Sverige e Watson, anche la normativa in discussione nel presente caso «riguarda in maniera generalizzata tutti gli abbonati ed utenti iscritti e ha ad oggetto tutti i mezzi di comunicazione elettronica nonché l'insieme dei dati relativi al traffico [e] non prevede alcuna differenziazione, limitazione o eccezione in funzione dell'obiettivo perseguito» [68]. Di conseguenza, «[e]ssa si applica (…) finanche a persone per le quali non esiste alcun

61 Articolo R. 10-13 del codice delle poste e delle comunicazioni elettroniche.

62 Sia la Quadrature del Net che la Fédération des fournisseurs d'accès à Internet associatifs sottolineano l'ampiezza delle finalità perseguite con la conservazione, il potere discrezionale riconosciuto alle autorità, l'assenza di criteri oggettivi nella loro definizione e la rilevanza attribuita a forme di criminalità che non possono essere qualificate come gravi.

63 La Commission nationale de contrôle des techniques de renseignement (Commissione nazionale di controllo delle tecniche di informazione, Francia). V., a tale proposito, punti da 145 a 148 delle osservazioni scritte del governo francese.

64 Punto 60 delle osservazioni scritte della Commissione.

65 In realtà, essi vanno un poco oltre, in quanto sembra che sia prevista, nel caso dei servizi di accesso a internet, anche la conservazione dell'indirizzo IP o dei codici di accesso.

66 Sentenza Tele2 Sverige e Watson, punto 100.

67 Ibidem, punto 107.

68 Ibidem, punto 105.

indizio di natura tale da far credere che il loro comportamento possa avere un nesso, sia pur indiretto o remoto, con violazioni penali gravi», e ciò senza ammettere alcuna eccezione, «di modo che essa si applica anche a persone le cui comunicazioni sono sottoposte, secondo le norme del diritto nazionale, al segreto professionale» [69].

116. Allo stesso modo, la normativa controversa «non richiede alcuna correlazione tra i dati di cui si prevede la conservazione e una minaccia per la sicurezza pubblica. In particolare, essa non è limitata ad una conservazione avente ad oggetto dati relativi ad un periodo di tempo e/o a una zona geografica e/o una cerchia di persone suscettibili di essere implicate in una maniera o in un'altra in una violazione grave, oppure persone che potrebbero, per altri motivi, contribuire, mediante la conservazione dei loro dati, alla lotta contro la criminalità» [70].

117. Da quanto precede si deduce che tale normativa «travalica (…) i limiti dello stretto necessario e non può essere considerata giustificata, in una società democratica, così come richiede 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» [71].

118. Quanto sopra è stato sufficiente affinché la Corte concludesse che le norme nazionali in questione non erano compatibili con l'articolo 15, paragrafo 1, della direttiva 2002/58, in quanto sancivano, «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» [72].

119. La questione che sorge ora è se la giurisprudenza della Corte in tema di conservazione di dati personali possa, se non essere rimessa in discussione, quanto meno temperata quando lo scopo perseguito con siffatta conservazione «generalizzata e indifferenziata» sia la lotta contro il terrorismo. La prima questione nella causa C-511/18 viene sollevata per l'appunto «in un contesto caratterizzato da minacce gravi e persistenti alla sicurezza nazionale, e in particolare dal rischio terroristico».

120. Tuttavia, se pure è questo il *contesto di fatto* in cui viene imposto l'obbligo di conservazione dei dati, certamente il suo *contesto normativo* non riguarda unicamente il terrorismo. Il regime di conservazione e di accesso ai dati in discussione nel procedimento dinanzi al Conseil d'État (Consiglio di Stato) subordina tale obbligo ai fini della ricerca, dell'accertamento e del perseguimento dei reati in generale.

121. Ad ogni modo, ricordo che la lotta contro il terrorismo non è rimasta al di fuori delle argomentazioni della sentenza Tele2 Sverige e Watson, ma la Corte ha ritenuto in quel caso che tale modalità criminale non richiedesse alcuna modulazione della sua giurisprudenza [73].

122. Pertanto, e in linea di principio, ritengo che alla questione del giudice del rinvio, incentrata sulla specificità della minaccia terroristica, debba rispondersi nello stesso senso in cui si è pronunciata la Corte nella sentenza Tele2 Sverige e Watson.

123. Come ho sostenuto nelle conclusioni nella causa Stichting Brein, «[i]l principio della certezza nell'applicazione del diritto impone agli organi giurisdizionali, se non l'applicazione dello stare decisis in termini assoluti, quanto meno la cautela di attenersi a quanto hanno statuito essi stessi, dopo attenta riflessione, su un determinato problema giuridico» [74].

69 Ibidem.

70 Sentenza Tele2 Sverige e Watson, punto 106.

71 Ibidem, punto 107.

72 Ibidem, punto 112.

73 Ibidem, punto 103.

74 C-527/15, EU:C:2016:938, paragrafo 41.

2) Conservazione dei dati limitata di fronte alle minacce contro la sicurezza dello Stato, compresa quella terroristica

124. Ciononostante, sarebbe possibile modulare o completare tale giurisprudenza, in considerazione delle sue conseguenze sulla lotta contro il terrorismo o sulla protezione dello Stato di fronte ad altre analoghe minacce contro la sicurezza nazionale?

125. Ho già sottolineato che la conservazione di dati personali implica di per sé un'ingerenza nei diritti garantiti dagli articoli 7, 8 e 11 della Carta [75]. A prescindere dal fatto che, in definitiva, ciò cui si mira con essa è rendere possibile l'*accesso*, retrospettivo o simultaneo, ai dati in un determinato momento [76], la conservazione di dati che vadano oltre lo stretto indispensabile per la trasmissione di una comunicazione o la fatturazione dei servizi prestati dal prestatore comporta di per sé l'inosservanza dei limiti previsti agli articoli 5 e 6 della direttiva 2002/58.

126. Gli utenti di tali servizi (in realtà, la quasi totalità dei cittadini delle società più sviluppate) godono, o devono godere, di una legittima aspettativa a che, in mancanza del loro consenso, non saranno conservati più dati che li riguardano rispetto a quelli archiviati conformemente a tali disposizioni. Le eccezioni di cui all'articolo 15, paragrafo 1, della direttiva 2002/58 devono essere interpretate muovendo da tale premessa.

127. Come ho già chiarito, nella sentenza Tele2 Sverige e Watson la Corte ha escluso, anche in relazione alla lotta contro il terrorismo, la conservazione generalizzata e indifferenziata dei dati personali [77].

128. Di fronte alle critiche ricevute, non credo che la dottrina elaborata in tale sentenza sottovaluti la minaccia terroristica, in quanto forma di criminalità particolarmente grave che comporta un'esplicita finalità di contestazione dell'autorità dello Stato e di destabilizzazione o distruzione delle sue istituzioni. La lotta al terrorismo è, letteralmente, vitale per lo Stato e il suo successo costituisce un obiettivo di interesse generale irrinunciabile per uno Stato di diritto.

129. Praticamente tutti i governi intervenuti nel procedimento, oltre alla Commissione, hanno osservato unanimemente che, al di là delle sue difficoltà tecniche, una conservazione parziale e diversificata dei dati personali priverebbe i servizi di intelligence nazionale della possibilità di accedere ad informazioni indispensabili per l'identificazione di minacce alla sicurezza pubblica e la difesa dello Stato, nonché per il perseguimento degli autori di attentati terroristici [78].

75 Come ha rammentato la Corte al punto 124 del parere 1/15, «la comunicazione di dati personali a un terzo, come un'autorità pubblica, costituisce un'ingerenza nel diritto fondamentale sancito all'articolo 7 della Carta indipendentemente dall'uso ulteriore delle informazioni comunicate. Lo stesso vale per la conservazione dei dati personali nonché per l'accesso agli stessi ai fini del loro uso da parte delle autorità pubbliche. A tal riguardo, poco importa 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 tale ingerenza».

76 Come osservato dall'avvocato generale Cruz Villalón nelle conclusioni nella causa Digital Rights, C-293/12 e C-594/12 (EU:C:2013:845, paragrafo 72), «la raccolta e soprattutto la conservazione, all'interno di gigantesche banche dati, di molteplici dati generati o trattati nell'ambito della maggior parte delle usuali comunicazioni elettroniche tra i cittadini dell'Unione costituisce una grave ingerenza nella loro vita privata, anche quando si limiti a creare le condizioni per un possibile controllo ex post delle loro attività personali e professionali. La raccolta di tali dati crea le condizioni per un controllo che, seppur esercitato soltanto a posteriori in occasione del loro impiego, minaccia tuttavia in modo permanente, per tutto il periodo della loro conservazione, il diritto dei cittadini dell'Unione alla riservatezza della loro vita privata. La diffusa sensazione di controllo così generata solleva in modo particolarmente acuto la questione del periodo di conservazione dei dati».

77 Sentenza Tele2 Sverige e Watson, punto 103: «non vale (…) a giustificare che una normativa nazionale che prevede la conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione venga considerata necessaria ai fini della lotta suddetta».

78 È questa l'interpretazione sostenuta, ad esempio, dal governo francese, il quale illustra tale affermazione con esempi concreti dell'utilità della conservazione generalizzata dei dati, che ha reso possibile la reazione dello Stato di fronte ai gravi attentati terroristici subiti dal suo paese negli ultimi anni (punti 107 e da 122 a 126 delle osservazioni scritte del governo francese).

130. Di fronte a tale valutazione mi sembra pertinente rilevare che la lotta contro il terrorismo non deve essere impostata solo pensando alla sua efficacia. Da ciò deriva la sua difficoltà, ma anche la sua grandezza quando i suoi mezzi e metodi rispettano i requisiti dello Stato di diritto, che significa anzitutto assoggettamento del potere e della forza ai limiti del diritto e, in particolare, a un ordinamento giuridico che trova nella difesa dei diritti fondamentali la ragione e il fine della sua esistenza.

131. Se per il terrorismo la giustificazione dei suoi mezzi non si basa su criteri diversi da quello della pura (e massima) efficacia dei suoi attacchi all'ordine costituito, per lo Stato di diritto l'efficacia si misura in termini che non consentono di prescindere, nella sua difesa, dalle procedure e garanzie che lo qualificano come un ordinamento legittimo. Se si abbandonasse semplicemente alla mera efficacia, lo Stato di diritto perderebbe la qualità che lo contraddistingue e potrebbe diventare esso stesso, in casi estremi, una minaccia per il cittadino. Nulla potrebbe assicurare che, dotando il potere pubblico di strumenti esorbitanti per il perseguimento dei reati, mediante i quali esso potesse ignorare o svuotare di contenuto i diritti fondamentali, la sua azione incontrollata e totalmente libera non si risolverebbe in definitiva in un pregiudizio alla libertà di tutti.

132. L'efficacia del potere pubblico, ripeto, trova una barriera insuperabile nei diritti fondamentali dei cittadini, le cui limitazioni, come prescritto dall'articolo 52, paragrafo 1, della Carta, possono essere introdotte solo per legge e rispettando il loro contenuto essenziale «laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui» [79].

133. Sulle condizioni alle quali, conformemente alla sentenza Tele2 Sverige e Watson, sarebbe ammissibile una conservazione *mirata* dei dati, rinvio alle mie conclusioni nella causa C-520/18 [80].

134. Circostanze nelle quali le informazioni disponibili in possesso dei servizi di sicurezza consentano di confermare il fondato sospetto che sia in preparazione un attentato terroristico possono costituire un caso legittimo di imposizione dell'obbligo di conservare taluni dati. A maggior ragione può esserlo l'effettiva commissione di un attentato. Se pure, in quest'ultimo caso, la perpetrazione del delitto può costituire di per una sé un fattore idoneo a giustificare l'adozione di detta misura, di fronte al mero sospetto di un eventuale attentato occorrerebbe che le circostanze che lo fondano presentassero un grado minimo di verosimiglianza, indispensabile per una ponderazione oggettiva degli indizi che possono giustificarla.

135. Seppur difficile, non è impossibile determinare con precisione e sulla base di criteri oggettivi sia le categorie di dati la cui conservazione è considerata imprescindibile, sia la cerchia degli interessati. Certamente, la soluzione più *pratica ed efficace* sarebbe la conservazione generale e indifferenziata di tutti i dati che possono essere raccolti dai fornitori di servizi di comunicazione elettronica, ma ho già rilevato che la questione non può essere risolta in termini di *efficacia pratica*, bensì di *efficacia giuridica*, e nel contesto di uno Stato di diritto.

136. Tale determinazione è tipicamente legislativa, nei limiti posti dalla giurisprudenza della Corte. Rinvio nuovamente a quanto espongo sul punto nelle conclusioni nella causa C-520/18 [81].

79 Sentenza del 15 febbraio 2016, N. (C-601/15 PPU, EU:C:2016:84, punto 50). Si tratta dunque del difficile equilibrio tra l'ordine pubblico e la libertà cui ho già fatto riferimento e al quale aspira per principio l'intera normativa dell'Unione. Si veda ad esempio la direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio (GU 2017, L 88, pag. 6). Pur prevedendo all'articolo 20, paragrafo 1, che gli Stati membri devono garantire che gli incaricati delle indagini o dell'azione penale per i reati di terrorismo «dispongano di strumenti di indagine efficaci», essa enuncia al considerando 21 che il ricorso a tali strumenti efficaci «dovrebbe essere mirato e tenere conto del principio di proporzionalità nonché della natura e della gravità dei reati oggetto d'indagine, e dovrebbe rispettare il diritto alla protezione dei dati personali».

80 Paragrafi da 87 a 95.

81 Paragrafi da 100 a 107.

3) Accesso ai dati conservati

137. Supponendo che gli operatori abbiano raccolto i dati secondo modalità compatibili con le disposizioni della direttiva 2002/58 e che la loro conservazione sia stata effettuata a norma dell'articolo 15, paragrafo 1, della stessa [82], l'accesso delle autorità competenti a tali informazioni deve avvenire nel rispetto delle condizioni richieste dalla Corte che, per quanto mi riguarda esamino nelle conclusioni nella causa C-520/18, alle quali rinvio [83].

138. Pertanto, anche nel presente caso la normativa nazionale deve prevedere i requisiti sostanziali e procedurali che disciplinano l'accesso delle autorità nazionali competenti ai dati conservati [84]. Nel contesto dei presenti rinvii pregiudiziali, tali requisiti autorizzerebbero l'accesso ai dati delle persone sospettate di progettare, di commettere o di aver commesso un atto terroristico o di esservi implicate [85].

139. Tuttavia, l'essenziale è che, salvo in casi di urgenza debitamente giustificati, l'accesso ai dati in questione sia soggetto al previo controllo di un organo giurisdizionale o di un'autorità amministrativa indipendente la cui decisione risponda a una richiesta motivata delle autorità competenti [86]. In tal modo, là dove non può giungere il giudizio in astratto della legge si garantisce il giudizio in concreto di detta autorità indipendente, cui spetta sia assicurare la sicurezza dello Stato sia tutelare i diritti fondamentali dei cittadini».

4) Obbligo di conservazione di dati che consentano di identificare gli autori di contenuti, alla luce della direttiva 2000/31 (seconda questione pregiudiziale nella causa C-512/18)

140. Il giudice del rinvio richiama la direttiva 2000/31 in quanto punto di riferimento per stabilire se si possano obbligare determinate persone [87] e agli operatori che offrono servizi di comunicazione al pubblico a conservare i dati che consentano «l'identificazione di chiunque abbia contribuito alla creazione del contenuto o di uno dei contenuti dei servizi da ess[i] prestati al fine di permettere all'autorità giudiziaria, se del caso, di richiederne la comunicazione per ottenere il rispetto delle norme in materia di responsabilità civile o penale».

141. Concordo con la Commissione nel ritenere che sarebbe fuori luogo esaminare la compatibilità di tale obbligo con la direttiva 2000/31 [88], dal momento che l'articolo 1, paragrafo 5, lettera b), di quest'ultima esclude dal suo ambito di applicazione le «questioni relative ai servizi della società dell'informazione oggetto delle direttive 95/46/CE e 97/66/CE», norme che corrispondono attualmente al regolamento 2016/679 e alla direttiva 2002/58 [89], i cui rispettivi articoli 23, paragrafo 1, e 15, paragrafo 1, devono essere interpretati, a mio avviso, nei termini sopra esposti.

82 Fermo restando che devono essere rispettate le condizioni indicate al punto 122 della sentenza Tele2 Sverige e Watson: la Corte ha ricordato che l'articolo 15, paragrafo 1, della direttiva 2002/58 non consente di derogare all'articolo 4, paragrafi 1 e 1 bis, della stessa, il quale esige che i fornitori prendano misure che consentano di garantire la protezione dei dati conservati contro il rischio di abusi, nonché contro l'accesso illecito. In tal senso, in detta sentenza è stato dichiarato che, «[t]enuto conto della quantità di dati conservati, del carattere sensibile dei dati stessi, nonché del rischio di accesso illecito a questi ultimi, i fornitori di servizi di comunicazione elettronica devono, al fine di assicurare la piena integrità e la riservatezza dei dati suddetti, garantire un livello particolarmente elevato di protezione e di sicurezza mediante misure tecniche e organizzative appropriate. In particolare, la normativa nazionale deve prevedere la conservazione nel territorio dell'Unione nonché la distruzione irreversibile dei dati al termine della durata di conservazione degli stessi».

83 Paragrafi da 52 a 60.

84 Sentenza Tele2 Sverige e Watson, punto 118.

85 Ibidem, punto 119.

86 Ibidem, punto 120.

87 Quelle che «garantiscono (…) mediante la messa a disposizione del pubblico tramite servizi di comunicazione al pubblico online, l'archiviazione di segnali, scritti, immagini, suoni o messaggi di qualsiasi natura forniti dai destinatari di detti servizi (…)».

88 Il giudice del rinvio menziona tale direttiva, in termini generali e senza richiamarne alcuna disposizione specifica, nella seconda questione sollevata nella causa C-512/18.

89 Punti 112 e 113 delle osservazioni scritte della Commissione.

2. Sull'obbligo di raccolta in tempo reale dei dati relativi al traffico e all'ubicazione (seconda questione pregiudiziale nella causa C-511/18)

142. Secondo il giudice del rinvio, l'articolo L. 851-2 del codice della sicurezza interna autorizza, esclusivamente al fine della prevenzione del terrorismo, la raccolta, in tempo reale, delle informazioni relative a persone precedentemente identificate come potenzialmente collegate a una minaccia terroristica. Allo stesso modo, l'articolo L. 851-4 di detto codice autorizza la trasmissione in tempo reale, da parte degli operatori, dei dati tecnici concernenti l'ubicazione delle apparecchiature terminali.

143. Secondo il giudice del rinvio, 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.

144. Inoltre, ai sensi dell'articolo L. 851-3 del codice della sicurezza interna, è possibile 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». Tale tecnica non comporta una conservazione generalizzata e indifferenziata dei dati ed è destinata alla raccolta, per un periodo limitato, di dati di connessione che potrebbero essere collegati ad un reato di natura terroristica.

145. A mio avviso, le condizioni richieste per l'accesso ai dati personali conservati devono essere applicate del pari all'accesso in tempo reale ai dati generati nel corso delle comunicazioni elettroniche. Rinvio, pertanto, a quanto osservato sul punto. È ininfluente che si tratti di dati conservati o di dati ottenuti sul momento, dato che in entrambi i casi viene presa conoscenza di dati personali, non rilevando che essi siano di carattere storico oppure attuali.

146. In pratica, qualora l'accesso in tempo reale sia conseguenza di connessioni individuate mediante un trattamento automatizzato, come quello previsto dall'articolo L. 851-3 del codice della sicurezza interna, occorre che i modelli e criteri prestabiliti per tale trattamento siano specifici, affidabili e non discriminatori, in modo da agevolare l'identificazione di soggetti di cui si può ragionevolmente sospettare la partecipazione ad attività terroristiche [90].

3. Sull'obbligo di informare gli interessati (terza questione nella causa C-511/18)

147. La Corte ha dichiarato che le autorità nazionali alle quali è stato consentito l'accesso ai dati devono informare gli interessati di tale circostanza, sempre che ciò non comprometta le indagini in corso. La ragione di tale obbligo è che detta informazione risulta necessaria per consentire agli interessati di esercitare il proprio diritto di ricorso, espressamente menzionato all'articolo 15, paragrafo 2, della direttiva 2002/58, in caso di violazione dei loro diritti [91].

148. Con la terza questione nella causa C-511/18, il Conseil d'État (Consiglio di Stato) chiede se tale obbligo di informazione sia vincolante in tutti i casi o vi si possa derogare quando siano previste altre garanzie, come quelle descritte da detto giudice nella sua decisione di rinvio.

90 Sentenza Digital Rights, punto 59.

91 Sentenza Tele2 Sverige e Watson, punto 121.

149. Secondo quanto esposto dal giudice a quo [92], le menzionate garanzie consistono nella possibilità per chi intenda accertare se una determinata tecnica di informazione è stata applicata in maniera illegittima di adire lo stesso Conseil d'État (Consiglio di Stato). Quest'ultimo potrebbe eventualmente annullare l'autorizzazione della misura e ordinare la distruzione dei dati raccolti, nell'ambito di un procedimento che non contempla il principio del contraddittorio tipico dei procedimenti giurisdizionali.

150. Il giudice del rinvio ritiene che tale normativa non violi il diritto a un ricorso effettivo. Tuttavia, sono dell'avviso che ciò si potrebbe ammettere, in teoria, per le persone che vogliano accertare se siano oggetto di un'operazione di intelligence. Viceversa, tale diritto non è rispettato se le persone che sono o sono state oggetto di una simile operazione non vengono avvertite di tale circostanza e, pertanto, non possono neppure chiedersi se i loro diritti siano stati violati o meno.

151. Le garanzie giurisdizionali alle quali fa riferimento il giudice del rinvio sembrano dipendere dall'iniziativa di chi sospetti di essere oggetto di una raccolta di informazioni sulla propria persona. Tuttavia, l'accesso al giudice per la tutela dei propri diritti deve essere effettivo per tutti, il che implica che chi abbia subìto un trattamento dei propri dati personali deve poter contestare giudizialmente la legittimità di tale trattamento e, di conseguenza, deve essere informato della sua esistenza.

152. È vero che, secondo quanto emerge dalle informazioni fornite, l'azione giurisdizionale può essere avviata d'ufficio o in virtù di una denuncia amministrativa, ma deve essere data all'interessato, in ogni caso, la possibilità di promuoverla egli stesso e tal fine occorre che gli sia comunicato che i suoi dati personali sono stati oggetto di un determinato trattamento. La difesa dei suoi diritti non può dipendere dalla circostanza che egli venga a conoscenza di tale trattamento tramite terzi o con i propri mezzi.

153. Pertanto, sempre che ciò non comprometta le indagini per le quali è stato consentito l'accesso ai dati conservati, la persona interessata deve essere informata di tale accesso.

154. Questione diversa è che, una volta che la persona interessata abbia avviato l'azione in giudizio, dopo essere stata informata dell'accesso ai suoi dati, il successivo procedimento giurisdizionale sia conforme ai requisiti di riservatezza e riserbo inerenti al controllo dell'azione dei poteri pubblici in settori sensibili come quello della difesa dello Stato. Tale questione, tuttavia, è estranea ai presenti rinvii, per cui non occorre, a mio avviso, che la Corte si pronunci al riguardo.

V. Conclusione

155. In considerazione di quanto precede, propongo alla Corte di rispondere al Conseil d'État (Consiglio di Stato, Francia) nei termini seguenti:

«L'articolo 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), in combinato disposto con gli articoli 7, 8, 11 e 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che:

1) Osta a una normativa nazionale che, in un contesto caratterizzato da minacce gravi e persistenti alla sicurezza nazionale, e in particolare dal rischio terroristico, impone agli operatori e ai fornitori di servizi di comunicazione elettronica di conservare, in maniera generale e indifferenziata, i dati relativi al traffico e all'ubicazione di tutti gli abbonati, nonché i dati che consentano di identificare gli autori dei contenuti offerti dai fornitori di detti servizi.

92 Punti da 8 a 11 della decisione di rinvio.

2) Osta a una normativa nazionale che non prevede l'obbligo di informare gli interessati del trattamento dei loro dati personali effettuato dalle autorità competenti, sempre che tale comunicazione non comprometta l'azione di dette autorità.

3) Non osta a una normativa nazionale che autorizza la raccolta in tempo reale dei dati relativi al traffico e all'ubicazione di singole persone, purché tale operazione si svolga secondo le procedure previste per l'accesso ai dati personali legittimamente conservati e con le medesime garanzie».