Raccolta della giurisprudenza

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

Causa C-623/17

Privacy International
contro
Secretary of State for Foreign and Commonwealth Affairs,
Secretary of State for the Home Department,
Government Communications Headquarters,
Security Service,
Secret Intelligence Service

[domanda di pronuncia pregiudiziale proposta dall'Investigatory Powers Tribunal (Tribunale competente per i poteri di indagine, Regno Unito)]

«Rinvio pregiudiziale – Trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche – Direttiva 2002/58/CE – Ambito di applicazione – Articolo 1, paragrafo 3 – Articolo 15, paragrafo 3 – Carta dei diritti fondamentali dell'Unione europea – Articoli 7, 8, 51 e 52, paragrafo 1 – Articolo 4, paragrafo 2, TUE – Trasmissione generalizzata e indifferenziata ai servizi di sicurezza dei dati di connessione degli utenti di un servizio di comunicazioni elettroniche»

1. Negli ultimi anni la Corte ha mantenuto una giurisprudenza 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;

– 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];

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

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).

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

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 tutela della sicurezza nazionale e per la lotta contro 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 i diritti relativi alla tutela della vita privata che essa protegge. Infine, si dovrà esaminare fino a che punto le diverse normative nazionali (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

5. Rinvio alla parte corrispondente delle mie conclusioni nelle cause C-511 e C-512/18.

B. Diritto nazionale (applicabile al caso di specie)

1. Telecommunications Act 1984 [11]

6. Ai sensi dell'articolo 94, un ministro può impartire a un operatore di una rete pubblica di comunicazioni elettroniche ordini generali o specifici che egli ritenga necessari nell'interesse della sicurezza nazionale o delle relazioni con il governo di un paese o territorio situato fuori dal Regno Unito.

2. Data Retention and Investigatory Powers Act 2014 [12]

7. L'articolo 1 così dispone:

«1) Il ministro può, tramite un avviso di conservazione, imporre a un operatore di telecomunicazioni pubbliche di conservare dati rilevanti relativi a comunicazioni, qualora ritenga che tale requisito sia necessario e proporzionato rispetto a una o più tra le finalità previste ai punti da a) ad h) dell'articolo 22, paragrafo 2, del Regulation of Investigatory Powers Act 2000 [legge del 2000 recante disciplina dei poteri di indagine; in prosieguo: il «RIPA»].

(2) Un avviso di conservazione può:

(a) riguardare un particolare operatore o qualsiasi categoria di operatori,

7 Oltre a quella presente, si tratta delle cause C-511/18 e C-512/18, La Quadrature du Net e a., e C-520/18, Ordre des barreaux francophones et germanophone e a.

8 Privacy International, C-623/17.

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

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

11 Legge del 1984 sulle telecomunicazioni; in prosieguo: la «legge del 1984».

12 Legge del 2014 sulla conservazione dei dati e sui poteri di indagine; in prosieguo: il «DRIPA».

(b) imporre la conservazione di tutti i dati o di qualsiasi categoria di dati;

(c) indicare il periodo o i periodi durante i quali i dati devono essere conservati;

(d) stabilire ulteriori prescrizioni o restrizioni in relazione alla conservazione dei dati;

(e) prevedere disposizioni diverse per finalità diverse;

(f) riguardare dati che siano o no esistenti al momento dell'emissione, o dell'entrata in vigore, dell'avviso.

(3) Il ministro può, tramite regolamenti, adottare ulteriori disposizioni in relazione alla conservazione dei dati pertinenti relativi alle comunicazioni.

(4) Tali disposizioni possono, in particolare, riguardare:

(a) requisiti antecedenti all'emissione dell'avviso di conservazione;

(b) il periodo massimo durante il quale i dati devono essere conservati in applicazione di un avviso di conservazione;

(c) il contenuto, l'emissione, l'entrata in vigore, il riesame, la modifica o la revoca di un avviso di conservazione;

(d) l'integrità, la sicurezza o la protezione dei dati conservati ai sensi del presente articolo, l'accesso ai dati, o la loro divulgazione o distruzione;

(e) l'attuazione di requisiti o restrizioni pertinenti, o la verifica della loro conformità;

(f) un codice di buone pratiche relativo ai requisiti o alle restrizioni pertinenti o ai poteri pertinenti;

(g) il rimborso da parte del ministro (subordinato o meno a condizioni) delle spese sostenute dagli operatori di telecomunicazioni pubbliche per ottemperare ai requisiti o alle restrizioni pertinenti;

(…)

(5) Il periodo massimo previsto ai sensi del paragrafo 4, lettera b), non deve eccedere i 12 mesi a partire dalla data indicata in relazione ai dati di cui trattasi dai regolamenti contemplati dal paragrafo 3.

(6) Un operatore di telecomunicazioni pubbliche che conservi dati pertinenti relativi a comunicazioni in applicazione del presente articolo non può divulgare tali dati, salvo che:

(a) li divulghi in conformità con:

(i) il capo 2 della parte 1 del [RIPA] o

(ii) una decisione giudiziaria o qualsiasi altra autorizzazione o mandato giudiziari, o che

(b) sia previsto dai regolamenti di cui al paragrafo 3.

(7) Il ministro può adottare, in via regolamentare, disposizioni corrispondenti a qualsiasi norma adottata (o adottabile) in applicazione del paragrafo 4, lettere da d) a g), o del paragrafo 6, in relazione ai dati relativi a comunicazioni conservati da fornitori di servizi di telecomunicazione in applicazione di un codice di buone pratiche ai sensi dell'articolo 102 dell'Anti-terrorism, Crime and Security Act 2001 [legge del 2001 sulla lotta al terrorismo, la criminalità e la sicurezza]».

3. RIPA

8. L'articolo 21 così dispone:

«(…)

(4) Nel presente capo, l'espressione "dati relativi a comunicazioni" può avere uno dei significati che seguono:

(a) i dati sul traffico riportati in una comunicazione o allegati ad essa (dal mittente o altrimenti) per le finalità di qualsiasi servizio postale o di qualsiasi sistema di telecomunicazione tramite il quale la comunicazione sia trasmessa o possa essere trasmessa;

(b) le informazioni che non ricomprendono nessuno dei contenuti di una comunicazione [ad eccezione delle informazioni di cui alla lettera a)], relative all'utilizzo effettuato da qualsiasi persona:

(i) di qualsiasi servizio postale o servizio di telecomunicazioni; o

(ii) in relazione alla fornitura o all'utilizzo da parte di qualsiasi persona di qualsivoglia servizio di telecomunicazioni, di qualsiasi parte di un sistema di telecomunicazioni;

(c) le informazioni che non rientrano nelle lettere (a) o (b), conservate o acquisite, in relazione ai destinatari del servizio, da una persona che presta un servizio postale o un servizio di telecomunicazioni.

(…)

(6) Nel presente articolo, l'espressione "dati sul traffico", in relazione a qualsiasi comunicazione, si riferisce a:

(a) qualsiasi dato che individui o sia idoneo a individuare la persona, l'apparecchio o l'ubicazione verso cui o da cui viene trasmessa o può essere trasmessa una comunicazione;

(b) qualsiasi dato che individui o selezioni oppure sia idoneo a individuare o selezionare l'apparecchio con cui viene trasmessa o può essere trasmessa la comunicazione;

(c) qualsiasi dato che includa segnali per l'attivazione dell'apparecchio utilizzato in un sistema di comunicazione ai fini della trasmissione di qualsiasi comunicazione; e

(d) qualsiasi dato che identifichi i dati riportati in una specifica comunicazione o allegati ad essa o altri dati come dati riportati in una specifica comunicazione o allegati ad essa.

(…)».

9. L'articolo 22 stabilisce quanto segue:

«(1) Il presente articolo si applica quando una persona responsabile ai fini del presente capo ritenga che sia necessario, per le ragioni elencate nel paragrafo 2 del presente articolo, ottenere qualsiasi dato relativo a comunicazioni.

(2) È necessario per ragioni ricadenti sotto il presente paragrafo ottenere i dati relativi a comunicazioni qualora questi ultimi siano necessari:

(a) nell'interesse della sicurezza nazionale;

(b) al fine di prevenire o accertare reati o di prevenire turbative all'ordine pubblico;

(c) nell'interesse del benessere economico del Regno Unito, sempreché tale interesse sia anche rilevante per gli interessi della sicurezza nazionale;

(d) nell'interesse della sicurezza pubblica;

(e) al fine della tutela della salute pubblica;

(f) al fine dell'accertamento o della riscossione di qualsiasi imposta, diritto, dazio o altro tributo, contributo o onere dovuti all'amministrazione pubblica;

(g) al fine di impedire, in caso di emergenza, la morte, le lesioni o qualsiasi danno alla salute fisica o psichica di una persona, o di attenuare qualsiasi lesione o danno alla salute fisica o psichica di una persona;

(h) per qualsiasi altro fine [non ricadente sotto le lettere da a) a g)] preciso in un'ingiunzione emessa dal ministro ai sensi dell'articolo 22, paragrafo 2, lettera h), del [DRIPA].

(4) Fatto salvo il paragrafo 5, qualora ritenga che un operatore di telecomunicazioni o un operatore postale sia in possesso, potrebbe essere in possesso o potrebbe entrare in possesso di dati, la persona responsabile può, con avviso all'operatore di telecomunicazioni o all'operatore postale, chiedere che tale operatore:

(a) ottenga i dati, ove questi non siano già in suo possesso, e

(b) in ogni caso, divulghi tutti i dati in suo possesso o che abbia successivamente ottenuto.

(5) La persona responsabile non deve rilasciare alcuna autorizzazione a norma del paragrafo 3, né emettere un avviso a norma del paragrafo 4, salvo che essa ritenga che l'acquisizione dei dati in questione in conseguenza di un comportamento autorizzato o imposto in virtù di un'autorizzazione o di un avviso sia proporzionata alla finalità perseguita tramite l'acquisizione dei dati».

10. Ai sensi dell'articolo 65, è possibile adire l'Investigatory Powers Tribunal (Tribunale competente per i poteri di indagine, Regno Unito) qualora vi sia motivo di ritenere che i dati siano stati ottenuti in maniera inadeguata.

II. Fatti e questioni pregiudiziali

11. Secondo il giudice del rinvio, il procedimento principale riguarda l'acquisizione e l'utilizzo di dati di comunicazione in massa da parte delle United Kingdom Security and Intelligence Agencies (agenzie di sicurezza e di intelligence del Regno Unito; in prosieguo: le «SIA»).

12. Tali dati si riferiscono a «chi» utilizza il telefono e Internet, e a «quando, dove, come e con chi». Essi includono l'ubicazione dei telefoni cellulari e di rete fissa dai quali sono effettuate o ricevute le chiamate nonché l'ubicazione dei computer utilizzati per accedere a Internet. Tali dati non includono il contenuto delle comunicazioni, che può essere ottenuto unicamente in forza di un provvedimento giudiziario.

13. La ricorrente nel procedimento principale (la Privacy International, organizzazione non governativa per la difesa dei diritti umani) ha proposto un ricorso dinanzi al giudice del rinvio, deducendo che l'acquisizione e l'utilizzo dei dati in parola da parte delle SIA costituirebbero violazione del diritto alla vita privata garantito dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (in prosieguo: la «CEDU») e sarebbero contrari al diritto dell'Unione.

14. Le autorità resistenti [13] replicano che l'esercizio delle loro competenze in materia è legittimo ed essenziale per motivi, inter alia, di tutela della sicurezza nazionale.

15. Secondo le informazioni contenute nell'ordinanza di rinvio, conformemente agli ordini impartiti dal ministro a norma dell'articolo 94 della legge del 1984, le SIA ricevono i dati di comunicazione in massa attraverso gli operatori di reti pubbliche di comunicazione elettronica.

16. Tali dati includono quelli relativi al traffico e all'ubicazione, nonché informazioni sulle attività sociali, commerciali e finanziarie, e sulle comunicazioni e i viaggi degli utenti. Le SIA conservano tali dati, una volta in loro possesso, in modo sicuro, utilizzando tecniche (per esempio, filtraggio e raggruppamento) non mirate, ossia non orientate a obiettivi specifici e noti.

17. Il giudice del rinvio ritiene accertato che tali tecniche sono essenziali per il compito delle SIA, consistente nel combattere le minacce gravi alla pubblica sicurezza, in particolare il terrorismo, lo spionaggio e la proliferazione delle armi nucleari. Le capacità delle SIA di acquisire e utilizzare i dati è fondamentale per la tutela della sicurezza nazionale del Regno Unito.

18. Secondo il giudice del rinvio, le misure controverse sono conformi al diritto interno e all'articolo 8 della CEDU. Esso dubita invece della loro compatibilità con il diritto dell'Unione, tenuto conto della sentenza Tele2 Sverige e Watson.

19. In tale contesto, detto giudice sottopone alla Corte le seguenti questioni pregiudiziali:

«1) Se, tenuto conto dell'articolo 4 TUE e dell'articolo 1, paragrafo 3, della direttiva 2002/58 (…), la prescrizione contenuta in un ordine rivolto da un ministro (Secretary of State) a un gestore di reti di comunicazione elettronica di fornire dati di comunicazione in massa alle agenzie di sicurezza e di intelligence ("SIA") di uno Stato membro rientri nell'ambito di applicazione del diritto dell'Unione e della direttiva [2002/58].

2) In caso di risposta affermativa alla prima questione, se al menzionato ordine ministeriale si applichi alcuna delle prescrizioni della sentenza Watson [14] o qualsiasi altra prescrizione oltre a quelle imposte dalla CEDU. In caso affermativo, in qual misura ed entro quali limiti si applichino tali prescrizioni, tenuto conto dell'esigenza fondamentale delle SIA di utilizzare tecniche di acquisizione in massa e di trattamento automatizzato per proteggere la sicurezza nazionale, e altresì in qual misura le capacità di cui trattasi, qualora altrimenti conformi alla CEDU, possano essere seriamente ostacolate dall'imposizione di dette prescrizioni».

13 Il Secretary of State for Foreign and Commonwealth Affairs (Ministro per gli Affari esteri e del Commonwealth), il Secretary of State for the Home Department (Ministro dell'Interno) e le tre SIA del Regno Unito, vale a dire i Government Communications Headquarters (sede governativa delle comunicazioni; GCHQ), il Security Service (servizi di sicurezza; MI5) e il Secret Intelligence Service (servizi di intelligence; MI6).

14 Id est, la giurisprudenza derivante dalla sentenza Tele2 Sverige e Watson.

20. Il giudice del rinvio contestualizza le sue questioni nei termini seguenti:

«a) le capacità [delle SIA] di usare [i dati di comunicazione in massa] di cui dispongono sono essenziali per la tutela della sicurezza nazionale del Regno Unito, anche ai fini di combattere il terrorismo, lo spionaggio e la proliferazione delle armi nucleari;

b) un aspetto fondamentale dell'utilizzo di [tali dati] da parte delle SIA consiste nel rilevare minacce alla sicurezza nazionale precedentemente ignote, attraverso tecniche di raccolta non mirate che si basano sull'aggregazione di [tali dati] in un unico luogo, la cui principale utilità consiste nell'individuazione e nell'elaborazione tempestiva di obiettivi, oltre a fornire una base d'azione a fronte di una minaccia imminente;

c) il fornitore di una rete di comunicazioni elettroniche non è successivamente tenuto a trattenere [tali dati] (oltre il periodo previsto per esigenze aziendali), che vengono quindi conservati unicamente dallo Stato (attraverso le SIA);

d) il giudice nazionale ha accertato (con talune riserve) che le garanzie relative all'uso di [tali dati] da parte delle SIA sono conformi con i requisiti imposti dalla CEDU; e

e) il giudice nazionale ha accertato che l'imposizione delle prescrizioni specificate [nella sentenza Tele2 Sverige e Watson], ove applicabili, vanificherebbe le misure adottate dalle SIA per proteggere la sicurezza nazionale, mettendo perciò a rischio la sicurezza del Regno Unito».

III. Procedimento dinanzi alla Corte

21. La domanda di pronuncia pregiudiziale è pervenuta presso la cancelleria della Corte il 31 ottobre 2017.

22. Hanno presentato osservazioni scritte i governi belga, ceco, cipriota, dei Paesi Bassi, del Regno Unito, estone, francese, irlandese, lettone, norvegese, polacco, portoghese, spagnolo, svedese, tedesco e ungherese, nonché la Commissione.

23. Il 9 settembre 2019 si è tenuta un'udienza pubblica, comune anche alle cause C-511/18, C-512/18 e C-520/18, alla quale hanno partecipato le parti dei quattro procedimenti pregiudiziali, i governi sopra menzionati, nonché la Commissione e il Garante europeo della protezione dei dati.

IV. Analisi

A. Sull'ambito di applicazione della direttiva 2002/58 e l'esclusione della sicurezza nazionale (prima questione pregiudiziale)

24. Nelle conclusioni che presento, anch'esse in data odierna, nelle cause C-511/18 e C-512/18, spiego i motivi per i quali, a mio avviso, 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» [15].

15 Conclusioni nelle cause C-511/18 e C-512/18, paragrafo 42.

25. Nello svolgimento della mia argomentazione, esamino l'incidenza delle sentenze della Corte del 30 maggio 2006, Parlamento/Consiglio e Commissione [16], e Tele2 Sverige e Watson, proponendo un'interpretazione che le integra entrambe [17].

26. Nelle medesime conclusioni, una volta affermata l'applicabilità della direttiva 2002/58, analizzo l'esclusione della sicurezza nazionale contemplata dalla stessa e l'incidenza dell'articolo 4, paragrafo 2, TUE [18].

27. Fatto salvo quanto esporrò in prosieguo, rinvio alle osservazioni svolte nelle suddette conclusioni e in quelle nella causa C-520/18.

1. L'applicazione della direttiva 2002/58 nella presente causa

28. Ai sensi delle norme controverse nella presente causa, i fornitori di servizi di comunicazione elettronica sono destinatari di un obbligo che implica, oltre alla conservazione, un trattamento dei dati in loro possesso in ragione del servizio che essi prestano agli utenti delle reti pubbliche di comunicazione dell'Unione [19].

29. Infatti, detti operatori devono trasmettere, obbligatoriamente, tali dati alle SIA. La questione sollevata nel caso di specie è se l'articolo 15, paragrafo 1, della direttiva 2002/58 consenta che siffatta trasmissione, tenuto conto del suo obiettivo, sia esclusa, sic et simpliciter, dall'ambito di applicazione del diritto dell'Unione.

30. Ritengo di no. La conservazione dei dati in parola e la loro successiva trasmissione possono essere qualificate come trattamento di dati personali effettuato dai fornitori di servizi di telecomunicazione elettronica, cosicché esse rientrano automaticamente nell'ambito di applicazione della direttiva 2002/58.

31. I motivi di sicurezza nazionale non possono essere anteposti a tale constatazione, come suggerito dal giudice del rinvio, con la conseguenza che l'obbligo controverso non rientrerebbe nella sfera di applicazione del diritto dell'Unione. A mio parere, ripeto, viene imposto ai fornitori un trattamento dei dati connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nell'Unione, che costituisce precisamente l'ambito della direttiva 2002/58, ai sensi del suo articolo 3, paragrafo 1.

32. Ciò posto, la discussione si incentra non già sulle attività delle SIA (che, come ho già rilevato, potrebbero collocarsi al di fuori del diritto dell'Unione qualora non riguardassero gli operatori di comunicazioni elettroniche), bensì sulla conservazione e la successiva trasmissione dei dati in possesso dei suddetti operatori. In quest'ottica, entrano in gioco i diritti fondamentali garantiti dall'Unione.

33. L'elemento chiave per dirimere tale discussione è, ancora una volta, l'obbligo di conservazione generalizzata e indifferenziata dei dati ai quali le autorità pubbliche possono accedere.

16 C-317/04 e C-318/04, EU:C:2006:346.

17 Conclusioni nelle cause C-511/18 e C-512/18, paragrafi da 44 a 76.

18 Ibidem, paragrafi da 77 a 90.

19 In virtù dell'articolo 2 della direttiva 2002/58, ai fini di tale direttiva si applicano le definizioni di cui alla direttiva 95/46. Ai sensi dell'articolo 2, lettera b), di quest'ultima, per «trattamento di dati personali» si intende «qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la *comunicazione mediante trasmissione*, diffusione o qualsiasi altra *forma di messa a disposizione*, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione» (il corsivo è mio).

2. Il richiamo alla sicurezza nazionale

34. Poiché nella presente causa il giudice del rinvio richiama in particolare l'attenzione sulle attività delle SIA che riguardano la sicurezza nazionale, mi permetto di riportare, al riguardo, alcuni paragrafi delle mie conclusioni che presento parimenti in data odierna nelle cause C-511/18 e C-512/18:

«77. La sicurezza nazionale (…) 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.

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". (…)

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.

(…)

82. Ritengo (…) che possa servire come orientamento il criterio della decisione quadro 2006/960/GAI (…), 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. (…)

(…)

84. Esiste (…) 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] considerando [11 della direttiva 2002/58] deriva dalla necessità di rispettare le competenze degli Stati membri in materia di sicurezza nazionale, allorché 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.

(…)

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».

3. Le conseguenze dell'applicazione al caso di specie della sentenza Tele2 Sverige e Watson

35. Il giudice del rinvio ha concentrato l'attenzione sull'interpretazione fornita dalla Corte nella sentenza Tele2 Sverige e Watson, facendo presenti le difficoltà che, a suo avviso, la sua applicazione al caso di specie comporterebbe.

36. La sentenza Tele2 Sverige e Watson ha indicato, infatti, le condizioni cui deve rispondere una normativa nazionale che introduca l'obbligo di conservare dati relativi al traffico e all'ubicazione ai fini del successivo accesso ai medesimi da parte delle autorità pubbliche.

37. Come nelle cause C-511/18 e C-512/18, e per analoghi motivi, ritengo che le norme nazionali sulle quali verte il presente rinvio non rispettino le condizioni definite nella sentenza Tele2 Sverige e Watson, in quanto implicano una conservazione generalizzata e indifferenziata di dati personali che fornisce un resoconto dettagliato della vita delle persone interessate per un lungo periodo di tempo.

38. Nelle conclusioni relative alle due cause suddette mi chiedo se si possa temperare o completare la giurisprudenza illustrata in tale sentenza, date le sue conseguenze sulla lotta al terrorismo o sulla protezione dello Stato contro altre minacce analoghe alla sicurezza nazionale.

39. Mi permetto inoltre di riportare di seguito alcuni paragrafi di dette conclusioni, nelle quali sostengo in sostanza che, pur potendosi temperare la succitata giurisprudenza, occorre confermarla nella sostanza:

«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 (…) 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. (…)

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 (…), l'accesso delle autorità competenti a tali informazioni deve avvenire nel rispetto delle condizioni richieste dalla Corte, che esamino nelle conclusioni nella causa C-520/18, alle quali rinvio.

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 (…). 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 (…).

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 (…). 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».

B. Sulla seconda questione

40. Il giudice del rinvio formula la sua seconda questione per l'ipotesi in cui si risponda alla prima in senso affermativo. In tal caso, esso chiede quale «altra prescrizione oltre a quelle imposte dalla CEDU» o derivanti dalla sentenza Tele2 Sverige e Watson debba applicarsi.

41. A tale proposito, esso afferma che l'imposizione dei requisiti di cui alla sentenza Tele2 Sverige e Watson «vanificherebbe le misure adottate dalle SIA per proteggere la sicurezza nazionale».

42. Poiché suggerisco di rispondere alla prima questione in senso negativo, non occorre esaminare la seconda. Quest'ultima, come evidenziato dallo stesso giudice del rinvio, è subordinata alla condizione che siano dichiarate compatibili con il diritto dell'Unione le «tecniche di acquisizione in massa e di trattamento automatizzato» dei dati personali di tutti gli utenti del Regno Unito, che gli operatori di servizi di comunicazione elettronica dovrebbero trasmettere alle SIA.

43. Qualora la Corte ritenesse necessario rispondere alla seconda questione, ritengo che dovrebbe confermare i menzionati requisiti della sentenza Tele2 Sverige e Watson per quanto riguarda:

– il divieto di accesso generalizzato ai dati;

– la necessità della previa autorizzazione di un organo giurisdizionale o di un'autorità indipendente per legittimare tale accesso;

– l'obbligo di informare gli interessati, salvo nel caso in cui ciò comprometta l'efficacia del provvedimento;

– la conservazione dei dati nell'Unione.

44. Sarebbe sufficiente, ripeto, confermare tali requisiti obbligatori per le ragioni che ho esposto nelle conclusioni relative alle cause C-511/18 e C-512/18 e C-520/18, senza che occorra introdurne «altri» aggiuntivi, nel senso indicato dal giudice del rinvio.

V. Conclusione

45. Alla luce delle considerazioni che precedono, propongo alla Corte di rispondere all'Investigatory Powers Tribunal (Tribunale competente per i poteri di indagine, Regno Unito) nei seguenti termini:

«L'articolo 4 TUE e l'articolo 1, paragrafo 3, 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), devono essere interpretati nel senso che ostano a una normativa nazionale che impone a un gestore di reti di comunicazione elettronica l'obbligo di fornire alle agenzie di sicurezza e di intelligence di uno Stato membro "dati di comunicazione in massa" che implicano la loro previa raccolta generalizzata e indifferenziata».

In subordine:

«L'accesso, da parte delle agenzie di sicurezza e di intelligence di uno Stato membro, ai dati trasmessi dai gestori di reti di comunicazione elettronica deve essere conforme ai requisiti stabiliti nella sentenza del 21 dicembre 2016, Tele2 Sverige e Watson (C-203/15 e C-698/15, EU:C:2016:970)».