Raccolta della giurisprudenza

CONCLUSIONI DELL'AVVOCATO GENERALE
MANUEL CAMPOS SÁNCHEZ-BORDONA
presentate il 30 marzo 2023 [1]

Causa C-162/22

A.G.
con l'intervento di:
Lietuvos Respublikos generalinė prokuratūra

[domanda di pronuncia pregiudiziale, proposta dallo Lietuvos vyriausiasis administracinis teismas (Corte amministrativa suprema, Lituania)]

«Rinvio pregiudiziale – Telecomunicazioni – Trattamento dei dati personali – Direttiva 2002/58/CE – Ambito di applicazione – Articolo 15, paragrafo 1 – Accesso ai dati conservati dai fornitori di servizi di comunicazione elettronica e raccolti nell'ambito di procedimenti di indagine – Uso successivo di dati nel corso di un'indagine su un illecito amministrativo»

1. Con il presente rinvio pregiudiziale si chiede, in sintesi, se alcuni dati personali ottenuti nel corso di un'indagine penale possano essere successivamente utilizzati in un procedimento disciplinare amministrativo nei confronti di un funzionario pubblico.

2. La risposta a questo interrogativo offre alla Corte una nuova occasione per pronunciarsi sui rispettivi ambiti di applicazione della direttiva 2002/58/CE [2], da un lato, e della direttiva (UE) 2016/680 [3] e del regolamento (UE) 2016/679 [4], dall'altro.

3. Per quanto riguarda la direttiva 2002/58, la Corte di giustizia ha elaborato una giurisprudenza, oramai consolidata, sui casi e sulle condizioni in cui gli Stati membri possono limitare la portata dei diritti e degli obblighi che essa stabilisce [5].

1 Lingua originale: lo spagnolo.

2 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).

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

4 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). In prosieguo: l'«RGPD».

5 A titolo esemplificativo, tra i principali riferimenti di questa giurisprudenza si possono citare le sentenze dell'8 aprile 2014, Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238); del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970); del 6 ottobre 2020, La Quadrature du Net e a. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791; in prosieguo: la «sentenza La Quadrature du Net»); del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche) (C-746/18, EU:C:2021:152), e del 5 aprile 2022, Commissioner of An Garda Síochána e a. (C-140/20, EU:C:2022:258; in prosieguo: la «sentenza Commissioner of An Garda Síochána»).

I. Contesto normativo

A. Diritto dell'Unione

1. Direttiva 2002/58

4. L'articolo 1 («Finalità e campo d'applicazione») afferma:

«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.

2. Ai fini di cui al paragrafo 1, le disposizioni della presente direttiva precisano e integrano la direttiva 95/46/CE [6]. Esse prevedono inoltre la tutela dei legittimi interessi degli abbonati che sono persone giuridiche.

3. La presente direttiva non si applica alle attività che esulano dal campo di applicazione del [TFUE], quali quelle disciplinate dai titoli V e VI del trattato sull'Unione europea [TUE] 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».

5. L'articolo 5 («Riservatezza delle comunicazioni»), paragrafo 1, prescrive:

«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».

6. L'articolo 15 («Applicazione di alcune disposizioni della direttiva 95/46/CE») afferma:

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

[6] 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).

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 [TUE].

(…)

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

(…)».

2. RGPD

7. L'articolo 2 («Ambito di applicazione materiale») così dispone:

«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;

(…)

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.

(…)».

8. L'articolo 5 («Principi applicabili al trattamento di dati personali») così recita:

«1. I dati personali sono:

(…)

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali ("limitazione della finalità");

(…)».

9. L'articolo 6 («Liceità del trattamento») stabilisce quanto segue:

«1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

(…)

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

(…)

3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:

a) dal diritto dell'Unione; o

b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento.

(...)

4. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;

b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;

c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;

d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;

(…)».

3. Direttiva 2016/680

10. L'articolo 1 («Oggetto e obiettivi»), paragrafo 1, così dispone:

«1. La presente direttiva stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica».

11. L'articolo 2 («Ambito di applicazione»), paragrafo 1, così recita:

«La presente direttiva si applica al trattamento dei dati personali da parte delle autorità competenti per le finalità di cui all'articolo 1, paragrafo 1».

12. L'articolo 4 («Principi applicabili al trattamento di dati personali») afferma:

«1. Gli Stati membri dispongono che i dati personali siano:

(…)

b) raccolti per finalità determinate, esplicite e legittime e trattati in modo non incompatibile con tali finalità;

(…)

2. Il trattamento da parte dello stesso o di un altro titolare del trattamento per una qualsiasi delle finalità di cui all'articolo 1, paragrafo 1, diversa da quella per cui sono raccolti i dati personali, è consentito nella misura in cui:

a) il titolare del trattamento è autorizzato a trattare tali dati personali per detta finalità conformemente al diritto dell'Unione o dello Stato membro; e

b) il trattamento è necessario e proporzionato a tale altra finalità conformemente al diritto dell'Unione o dello Stato membro.

(…)».

13. L'articolo 9 («Condizioni di trattamento specifiche»), paragrafo 1, così recita:

«I dati personali raccolti dalle autorità competenti per le finalità di cui all'articolo 1, paragrafo 1, non possono essere trattati per finalità diverse da quelle di cui all'articolo 1, paragrafo 1, a meno che tale trattamento non sia autorizzato dal diritto dell'Unione o dello Stato membro. Qualora i dati personali siano trattati per tali finalità diverse, si applica il [RGPD], a meno che il trattamento non sia effettuato nell'ambito di un'attività che non rientra nell'ambito di applicazione del diritto dell'Unione».

B. Diritto nazionale

1. Lietuvos Respublikos elektroninių ryšių įstatymas [7]

14. L'articolo 65, paragrafo 2, impone ai fornitori di servizi di comunicazione elettronica l'obbligo di conservare i dati elencati di cui all'allegato 1 della stessa legge e, se del caso, di metterli a disposizione delle autorità competenti affinché possano utilizzarli nella lotta alla criminalità grave [8].

15. Ai sensi dell'articolo 77, paragrafo 1, i fornitori di servizi di comunicazione elettronica devono fornire alle autorità competenti le informazioni in loro legittimo possesso necessarie, in particolare, per la prevenzione, l'accertamento e il perseguimento di reati.

16. A norma dell'articolo 77, paragrafo 4, se esiste una decisione giudiziaria motivata o un'altra base giuridica prevista dalla legge, i fornitori di servizi di comunicazione elettronica devono rendere tecnicamente possibile, in particolare agli organi di indagine penale e alle autorità istruttorie, secondo le modalità previste dal diritto processuale penale, il controllo del contenuto delle comunicazioni diffuse dalle reti di comunicazione elettronica.

2. Lietuvos Respublikos kriminalinės žvalgybos įstatymas [9]

17. Ai sensi dell'articolo 6, paragrafo 3, punto 1), se sono soddisfatte le condizioni stabilite dalla stessa LIC e previa autorizzazione del pubblico ministero o di un'autorità giudiziaria, gli organi di indagine penale [10] possono ottenere informazioni dai fornitori di servizi di comunicazione elettronica.

18. A norma dell'articolo 8, paragrafi 1 e 3, gli organi di indagine penale devono agire non appena siano disponibili informazioni relative alla preparazione o alla commissione di un reato molto grave, grave o relativamente grave, e, se l'indagine rivela l'esistenza di un reato, deve essere avviata immediatamente un'istruttoria penale.

19. Conformemente all'articolo 19, paragrafo 1, punto 5, le informazioni provenienti da operazioni di indagine penale possono essere utilizzate nei casi previsti dai paragrafi 3 e 4 del medesimo articolo, e negli altri casi previsti dalla legge.

20. Ai sensi dell'articolo 19, paragrafo 3, le informazioni relative a un fatto che presenta le caratteristiche di un reato di natura corruttiva possono essere declassificate, d'intesa con la Procura, e utilizzate nell'ambito di un'indagine su illeciti disciplinari o di servizio.

7 Legge della Repubblica di Lituania sulle comunicazioni elettroniche, nella versione della legge n. IX-2135 del 15 aprile 2004, modificata dalla legge n. XIII-2172 del 6 giugno 2019; in prosieguo: la «LCE».

8 I dati elencati in detto allegato («Categorie di dati da proteggere») sono quelli necessari per identificare l'origine e la destinazione di una comunicazione, la data, l'ora e la durata, il tipo di comunicazione e la localizzazione dello strumento di comunicazione (compresa la comunicazione mobile) degli utenti.

9 Legge della Repubblica di Lituania sull'intelligence criminale, nella versione della legge n. XI-2234 del 2 ottobre 2012, modificata dalla legge n. XIII-1837 del 20 dicembre 2018; in prosieguo: «LIC».

10 Userò il termine «informazioni», e non «intelligence», per designare i servizi che conducono le indagini corrispondenti.

3. Lietuvos Respublikos baudžiamojo proceso kodeksas [11]

21. Ai sensi dell'articolo 154, paragrafo 1 («Controllo, registrazione e conservazione delle informazioni trasmesse sulle reti di comunicazione elettronica»), un inquirente può, su provvedimento di un giudice istruttore adottato su richiesta del pubblico ministero, ascoltare, captare e conservare le conversazioni trasmesse attraverso reti di comunicazione elettronica se vi è motivo di ritenere che si possano ottenere informazioni su un reato molto grave o grave in fase di preparazione, di commissione o che è già stato commesso, o su un reato relativamente grave o non grave.

22. Ai sensi dell'articolo 177, paragrafo 1 («Divieto di divulgazione dei dati delle indagini preliminari»), i dati istruttori sono riservati e, fino alla fase giudiziale della causa, possono essere divulgati solo con l'autorizzazione della procura e solo nella misura in cui ciò sia giustificato [12].

II. Fatti, procedimento e questione pregiudiziale

23. La Lietuvos Respublikos generalinė prokuratūra (Procura generale della Repubblica di Lituania; in prosieguo: la «Procura generale») ha avviato un'indagine interna sull'operato di A.G., all'epoca procuratore presso una Apygardos prokuratūra (Procura regionale), in presenza di indizi di condotta illecita nell'esercizio di funzioni pubbliche.

24. La Commissione della Procura generale ha constatato che A.G. si è reso responsabile di condotta illecita nell'esercizio di funzioni pubbliche e ha proposto di infliggergli la sanzione disciplinare di rimozione da tali funzioni.

25. Detta condotta sarebbe stata accertata sulla base delle informazioni, ottenute nel corso dell'indagine amministrativa, derivanti dalle attività dei servizi di informazione criminale, dalle spiegazioni di altri funzionari e del ricorrente, nonché dalle risultanze di due indagini preliminari.

26. In particolare, vi sarebbero state comunicazioni telefoniche tra A.G. e il legale di un indagato nel corso di un'indagine preliminare condotta da A.G. riguardo a procedimenti in cui l'avvocato aveva agito in qualità di difensore [13].

27. Il controllo e la registrazione delle informazioni trasmesse attraverso le reti di comunicazione elettronica erano stati autorizzati mediante ordinanze del giudice.

28. Il procuratore generale ha inflitto la sanzione della rimozione dalle funzioni ad A.G., il quale ha presentato ricorso al Vilniaus apygardos administracinis teismas (Tribunale amministrativo regionale di Vilnius, Lituania), chiedendone l'annullamento.

[11] Codice di procedura penale della Repubblica di Lituania del 14 marzo 2002, nella versione applicabile al procedimento principale; in prosieguo: il «CPP».

[12] Secondo le Ikiteisminio tyrimo duomenų teikimo ir panaudojimo ne baudžiamojo persekiojimo tikslais ir ikiteisminio tyrimo duomenų apsaugos rekomendacijos (Raccomandazioni sulla fornitura e l'uso dei dati delle indagini preliminari a fini diversi dal perseguimento di reati e sulla protezione dei dati delle indagini preliminari) approvate con ordinanza del procuratore generale n. 1 279 del 17 agosto 2017, modificato con ordinanza n. 1 211 del 25 giugno 2018, in particolare la clausola 23, una volta ricevuta la richiesta di accesso ai dati istruttori, il procuratore decide se renderli disponibili. In caso affermativo, deve specificare in che modo possono essere forniti.

[13] Secondo quanto esposto in udienza, per tali fatti, i procedimenti penali nei confronti di A.G. e dell'avvocato sono ancora pendenti.

29. Il ricorso è stato respinto con sentenza del 16 luglio 2021, in quanto il giudice di primo grado ha ritenuto legittime le attività dei servizi di informazione criminale e l'utilizzo, nel corso del procedimento disciplinare, dei dati ottenuti da tali servizi.

30. A.G. ha proposto appello contro la sentenza di primo grado dinanzi allo Lietuvos vyriausiasis administracinis teismas (Corte amministrativa suprema, Lituania), che sottopone alla Corte di giustizia la presente questione pregiudiziale:

«Se l'articolo 15, paragrafo 1, della direttiva 2002/58/CE (…), in combinato disposto con gli articoli 7, 8, 11 e 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea [Carta], debba essere interpretato nel senso che esso vieti alle autorità pubbliche competenti di utilizzare, nell'ambito di indagini per condotta illecita di natura corruttiva nell'esercizio di funzioni pubbliche, i dati conservati dai fornitori di servizi di comunicazione elettronica che possono fornire informazioni sui dati di un utente di un mezzo di comunicazione elettronica e sulle comunicazioni da questi effettuate, indipendentemente dal fatto che l'accesso a tali dati sia stato concesso, nel caso concreto, ai fini del contrasto di reati gravi e di prevenzione di gravi minacce alla sicurezza pubblica».

III. Procedimento dinanzi alla Corte di giustizia

31. La domanda di pronuncia pregiudiziale è pervenuta alla cancelleria della Corte di giustizia il 3 marzo 2022.

32. Hanno presentato osservazioni scritte A.G., i governi ceco, estone, ungherese, irlandese, italiano e lituano, nonché la Commissione europea.

33. All'udienza, tenutasi il 2 febbraio 2023, sono comparsi A.G., i governi francese, ungherese, irlandese e lituano, nonché la Commissione.

IV. Valutazione

A. Ammissibilità. Delimitazione della risposta alla questione pregiudiziale

34. Il giudice del rinvio è un giudice amministrativo competente per il controllo giurisdizionale delle decisioni anche amministrative. Questa è la natura della decisione adottata dal procuratore generale, che ha inflitto la sanzione della revoca dalle funzioni a un funzionario di una procura territoriale, per fatti che costituiscono un illecito nell'esercizio delle sue funzioni.

35. La controversia di cui trattasi non verte, pertanto, sulle decisioni delle autorità giudiziarie penali. Anche se dette decisioni coesistono con il procedimento amministrativo (disciplinare) che ha dato origine alla revoca dalle funzioni [14], occorre sottolineare che la controversia sorge solo per quanto riguarda quest'ultima.

36. Ciò premesso, dalla decisione di rinvio emerge una certa imprecisione quanto ai fatti della controversia, che delineano il contesto in cui si colloca la questione pregiudiziale.

[14] V. nota 13 delle presenti conclusioni.

37. Come hanno sottolineato il governo ceco e la Commissione, non è possibile stabilire con certezza, sulla base dell'ordinanza di rinvio, se le autorità competenti: a) si siano rivolte ai fornitori di servizi di comunicazione elettronica per ottenere i dati controversi, o b) abbiano ottenuto esse stesse, direttamente, tali dati.

38. La questione non è affatto secondaria. Da essa dipende l'individuazione di quale normativa dell'Unione sia pertinente per rispondere alla questione pregiudiziale. A seconda che i fatti si siano verificati in un modo o nell'altro, deve essere applicata:

– la direttiva 2002/58, se i dati ottenuti sono il risultato di un obbligo di trattamento imposto ai fornitori di servizi di comunicazione elettronica; o

– la direttiva 2016/680, se i dati sono stati ottenuti direttamente dall'autorità pubblica, senza imporre obblighi a detti fornitori.

39. In questa seconda ipotesi, la protezione dei dati personali sarebbe disciplinata dal diritto nazionale, fatta salva l'applicazione della direttiva 2016/680[15]. La questione pregiudiziale, pertanto, ponendo l'accento sulla direttiva 2002/58, darebbe atto di un approccio inadeguato.

40. Il governo ungherese, convinto che i dati personali siano stati ottenuti attraverso operazioni di intercettazione telefonica effettuate dai servizi di informazione criminale, mette in dubbio la ricevibilità del rinvio pregiudiziale, in quanto la direttiva 2002/58 sarebbe, per le ragioni esposte, inapplicabile.

41. Per la Commissione, tuttavia,

– si applicherebbe la direttiva 2016/680 nella misura in cui si tratta di utilizzare, ai fini di un'indagine successiva, dati personali raccolti e conservati direttamente dalle autorità nel corso di un'indagine penale preliminare;

– si applicherebbe la direttiva 2002/58 se, come indicato dal giudice del rinvio[16], la raccolta e la conservazione di almeno una parte dei dati si è dovuta effettuare in forza di una norma nazionale adottata ai sensi dell'articolo 15, paragrafo 1, di tale direttiva. La direttiva 2002/58 sarebbe dunque pertinente per la risoluzione della controversia.

42. Concordo con questo approccio della Commissione che, peraltro, è l'unico che consenta di superare le perplessità (giustificate) generate dalla decisione di rinvio quanto alla sua ricevibilità.

43. Così intesa la questione pregiudiziale la pertinenza della direttiva 2002/58 ai fini della risposta a detta questione:

– deriva dalla presunzione, implicita in qualsiasi rinvio pregiudiziale, della necessità della sua formulazione, la cui responsabilità ricade sul giudice che la propone[17];

[15] Sentenza La Quadrature du Net, punto 103: «quando gli Stati membri attuano direttamente misure che derogano alla riservatezza delle comunicazioni elettroniche, senza imporre obblighi di trattamento ai fornitori di detti servizi di comunicazione, la protezione dei dati delle persone interessate non ricade nell'ambito della direttiva 2002/58, bensì unicamente in quello del diritto nazionale, fatta salva l'applicazione della [direttiva 2016/680]».

[16] Punto 37 dell'ordinanza di rinvio.

[17] Per tutte, sentenze del 4 dicembre 2018, Minister for Justice and Equality e Commissioner of An Garda Síochána (C-378/17, EU:C:2018:979), punto 26, e del 22 dicembre 2022, Airb-nb Ireland e Airbnb Payments UK (C-83/21, EU:C:2022:1018), punto 82.

– è ammissibile nella misura in cui l'interpretazione della Corte di giustizia è richiesta solo per quanto riguarda la direttiva 2002/58, che l'organo giurisdizionale ritiene essenziale per dirimere la controversia [18].

44. Infatti, secondo il giudice del rinvio, per il procedimento di cui è investito, sono rilevanti:

«i) l'accesso ai *dati conservati dai fornitori di servizi di comunicazione elettronica*, non solo ai fini del contrasto dei reati gravi e della prevenzione di gravi minacce alla sicurezza pubblica, e

ii) l'*uso dei dati conservati* ottenuti ai fini del contrasto dei reati gravi e della prevenzione di gravi minacce alla sicurezza pubblica nell'ambito delle indagini per condotta illecita di natura corruttiva nell'esercizio di funzioni pubbliche» [19].

45. Tutto sembrerebbe pertanto indicare che, al di fuori dell'eventuale concorso di dati personali il cui trattamento non potrebbe rientrare nell'ambito di applicazione della direttiva 2002/58 (ma in quello della direttiva 2016/680), nell'indagine che ha portato alla sanzione inflitta siano stati utilizzati dati personali raccolti presso i fornitori di servizi di comunicazione elettronica.

46. La risposta della Corte di giustizia deve essere circoscritta alla richiesta del giudice del rinvio come da quest'ultimo formulata. Occorre pertanto chiarire se i dati personali ottenuti e trattati sulla base dell'articolo 15, paragrafo 1, della direttiva 2002/58 nell'ambito di un'indagine penale possano essere successivamente utilizzati in un procedimento disciplinare (amministrativo) nei confronti di un funzionario pubblico.

47. Avendo così delimitato i termini del rinvio pregiudiziale, si può affermare, a contrario, che esulano dall'ambito dello stesso le seguenti questioni:

– in primo luogo, quelle sulla legittimità dell'*acquisizione* iniziale dei dati personali ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58. La questione del giudice del rinvio si limita all'*uso successivo* di tali dati nel procedimento disciplinare, senza mettere in discussione la legittimità della loro acquisizione originaria [20];

– in secondo luogo, quelle sull'uso di dati ottenuti e trattati direttamente dalle autorità pubbliche nel corso di precedenti indagini penali. Anche su questo punto, la cui disciplina rientra nell'ambito di applicazione del diritto nazionale e della direttiva 2016/680, il giudice del rinvio non solleva alcun dubbio.

[18] Il riferimento inequivocabile alla direttiva 2002/58 nel dispositivo della decisione di rinvio e il silenzio sulla direttiva 2016/680 nella sua argomentazione giuridica vanno nella stessa direzione. Diverso è il caso in cui la Corte di giustizia, pur senza superare i limiti della domanda, possa fornire al giudice del rinvio indicazioni utili per la sua decisione, eventualmente facendo ricorso ad altre norme del diritto dell'Unione. V., in tal senso, sentenza del 18 settembre 2019, VIPA (C-222/18, EU:C:2019:751), punto 50 e giurisprudenza ivi citata.

[19] Punto 35 dell'ordinanza di rinvio. Il corsivo è mio.

[20] Non è dunque necessario che la Corte di giustizia si pronunci sulla legittimità di dette operazioni preliminari. Se lo facesse, essa dovrebbe ribadire che l'*accesso* ai dati in possesso dei fornitori di servizi di comunicazione elettronica può essere concesso solo se la loro *conservazione* è conforme all'articolo 15, paragrafo 1, della direttiva 2002/58. V., in tal senso, la sentenza La Quadrature du Net, punto 167. Detto articolo, letto alla luce degli gli articoli 7, 8, 11 e 52, paragrafo 1, della Carta, osta a misure legislative che prevedono, a tali fini, a titolo preventivo, la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione (sentenza La Quadrature du Net, punto 168).

48. In sintesi, le considerazioni nel merito che seguono dovranno tralasciare l'interpretazione della direttiva 2016/680 [21]. Esse si limiteranno, per quanto riguarda la direttiva 2002/58, all'utilizzo dei dati personali ottenuti ai sensi della stessa mediante operazioni di trattamento di cui si deve presupporre la legittimità iniziale, dal momento che quest'ultima non viene contestata nel procedimento principale.

B. Nel merito

1. Sintesi della giurisprudenza della Corte di giustizia sull'applicazione della direttiva 2002/58

49. Dall'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58 si deduce che gli Stati membri possono adottare una misura che deroga al principio della riservatezza sancito dall'articolo 5, paragrafo 1, della stessa direttiva qualora essa sia «necessaria, opportuna e proporzionata all'interno di una società democratica», e risulti «strettamente» proporzionata allo scopo perseguito [22].

50. In particolare, la possibilità per gli Stati membri di giustificare una limitazione dei diritti e degli obblighi previsti agli articoli 5, 6 e 9 della direttiva 2002/58 deve essere valutata alla luce della gravità dell'ingerenza che una restrizione siffatta comporta e verificando che l'importanza dell'obiettivo di interesse generale perseguito da tale limitazione sia adeguata a detta gravità [23].

51. «Per soddisfare il requisito di proporzionalità, una normativa deve prevedere norme chiare e precise che disciplinino la portata e l'applicazione della misura considerata e fissino un minimo di requisiti, di modo che le persone i cui dati personali sono oggetto di attenzione dispongano di garanzie sufficienti che consentano di proteggere efficacemente tali dati contro i rischi di abuso. Tale normativa deve essere giuridicamente vincolante nell'ambito dell'ordinamento nazionale e, in particolare, indicare in quali circostanze e a quali condizioni una misura che prevede il trattamento di siffatti dati possa essere adottata (…)» [24].

52. Per quanto riguarda i motivi d'interesse generale che possono giustificare una misura adottata ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58, secondo il principio di proporzionalità esiste una gerarchia di obiettivi in funzione della loro rispettiva importanza: l'importanza dell'obiettivo perseguito da una simile misura deve essere rapportata alla gravità dell'ingerenza [25].

53. In questa gerarchia di obiettivi, la salvaguardia della sicurezza nazionale, letta alla luce dell'articolo 4, paragrafo 2, TUE, supera quella degli altri obiettivi di cui all'articolo 15, paragrafo 1, della direttiva 2002/58, vale a dire la difesa, la sicurezza pubblica o la prevenzione, la

[21] Tuttavia, vi farò riferimento, in via subordinata, nella parte finale delle presenti conclusioni.

[22] Sentenza La Quadrature du Net, punto 129.

[23] Sentenza La Quadrature du Net, punto 131, e giurisprudenza ivi citata.

[24] Sentenza Commissioner of An Garda Síochána, punto 54.

[25] Sentenza Commissioner of An Garda Síochána, punto 56.

ricerca, l'accertamento e il perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. L'obiettivo di lotta alla criminalità in generale, anche grave, e di salvaguardia della sicurezza pubblica rientra in quest'ultima categoria [26].

54. Da questa classificazione degli obiettivi consegue che:

– quello della salvaguardia della sicurezza nazionale, che è il primo nell'ordine gerarchico indicato dalla Corte di giustizia, consente ingerenze gravi quanto quelle rappresentate da misure legislative che consentono di imporre ai fornitori di servizi di comunicazione elettronica l'obbligo di conservare in maniera generalizzata e indifferenziata i dati relativi al traffico e i dati relativi all'ubicazione [27];

– l'obiettivo immediatamente successivo per importanza, vale a dire la lotta alle forme gravi di criminalità, può giustificare ingerenze quali, ad esempio, la conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione o degli indirizzi IP attribuiti all'origine di una connessione, per un periodo temporalmente limitato allo stretto necessario [28].

2. Applicazione della suddetta giurisprudenza nel presente rinvio pregiudiziale

55. Secondo il giudice del rinvio, i dati controversi sarebbero stati ottenuti mediante gravi ingerenze nei diritti garantiti dagli articoli 7, 8 e 11 della Carta [29].

56. Non si tratta qui, ripeto, di esaminare la legittimità iniziale dell'acquisizione di tali dati, vale a dire, di valutare se l'ingerenza sia stata sufficientemente giustificata in considerazione della gravità del reato contro cui si intendeva agire.

57. Su entrambi i punti (gravità dell'ingerenza e gravità del reato), si è pronunciato il giudice del rinvio in termini che non sono argomentati nel procedimento principale e non sono dunque pertinenti ai fini del rinvio pregiudiziale.

58. Ciò che rileva in questa sede, come espone il giudice del rinvio, è stabilire se quei dati: a) possano essere utilizzati anche nell'ambito di indagini successive finalizzate alla lotta contro la criminalità in generale (ipotizzando che la condotta oggetto della sanzione disciplinare controversa rientri in questa nozione), o b) possano essere utilizzati solo nell'ambito di indagini finalizzate alla lotta contro la criminalità grave.

59. I governi ceco e irlandese hanno esaminato se la condotta in causa dinanzi al giudice del rinvio meriti o meno di essere considerata un «reato grave» e hanno concluso in senso affermativo.

[26] Sentenza La Quadrature du Net, punti 135 e 136, in cui si spiega che la sicurezza nazionale costituisce una responsabilità esclusiva dello Stato che corrisponde all'interesse primario di tutelare le funzioni essenziali dello Stato e gli interessi fondamentali della società contro attività tali da destabilizzare gravemente le strutture costituzionali, politiche, economiche o sociali fondamentali di un paese, e in particolare da minacciare direttamente la società, la popolazione o lo Stato in quanto tale, quali in particolare le attività di terrorismo. Minacce che si distinguono, per la loro natura e particolare gravità, dal rischio generale che si verifichino tensioni o perturbazioni, anche gravi, della pubblica sicurezza. Ne consegue che l'obiettivo di salvaguardia della sicurezza nazionale è quindi idoneo a giustificare misure che comportino ingerenze nei diritti fondamentali più gravi di quelle che potrebbero legittimare tali altri obiettivi.

[27] Sentenza Commissioner of An Garda Síochána, punto 58.

[28] Sentenza La Quadrature du Net, punto 168.

[29] Così si evince dal punto 46 dell'ordinanza di rinvio: in quest'ultima si fa riferimento a dati che possono fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali utilizzate da tale utente e che consentono di trarre conclusioni precise riguardo alla vita privata delle persone interessate.

60. A mio avviso, si tratta tuttavia di un punto su cui la Corte di giustizia non deve pronunciarsi, poiché la qualificazione della condotta rientra nella competenza del giudice del rinvio.

61. Il giudice del rinvio afferma che, se l'uso di dati ottenuti mediante una grave ingerenza nei diritti fondamentali può essere giustificato solo nella lotta contro la criminalità grave e nella prevenzione contro gravi minacce alla sicurezza pubblica, non sarebbe possibile utilizzare questi dati nell'ambito di indagini su illeciti disciplinari di natura corruttiva [30], vale a dire, in indagini come quella controversa nella presente causa.

62. Sulla base di tale valutazione, ciò che interessa è stabilire se gli illeciti disciplinari per il cui perseguimento si vorrebbero utilizzare determinati dati personali devono essere qualitativamente equivalenti, in termini di gravità, agli illeciti che hanno giustificato la raccolta di tali dati [31].

63. In udienza, il governo lituano ha riconosciuto che la revoca dalle funzioni era stata imposta a causa di un illecito deontologico del procuratore sanzionato. Valutare se tale illecito (la fuga di notizie su un'indagine preliminare) possa essere assimilata a un reato grave o comporti un rischio grave per la salvaguardia della sicurezza pubblica dipende da una serie di fattori che solo il giudice del rinvio è in grado di verificare [32].

64. Nel corso dell'udienza sono stati fatti numerosi riferimenti alla lotta alla corruzione, come fenomeno alla base di condotte come quella oggetto del presente procedimento. Il dibattito su questo punto richiederebbe non poche puntualizzazioni, nell'interesse del rigore esigibile in tutte le manifestazioni del potere punitivo dello Stato. Occorrerebbe stabilire, ad esempio, se il termine «corruzione» sia usato in senso generico o si riferisca a un tipo specifico di comportamento nel quale, in astratto, sarebbe forse eccessivo includere la mera violazione del dovere di segretezza se non è accompagnata da un correlativo vantaggio a favore del funzionario [33].

65. In ogni caso, se il giudice del rinvio dovesse ritenere che l'illecito deontologico qui sanzionato sia di minore gravità rispetto al reato la cui indagine ha giustificato la misura adottata ai sensi dell'articolo 15 della direttiva 2002/58, la risposta alla sua questione pregiudiziale si desume dalle seguenti affermazioni della Corte:

– «[l]'accesso a dati relativi al traffico e a dati relativi all'ubicazione conservati da fornitori in applicazione di una misura adottata ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58, che deve avvenire nel pieno rispetto delle condizioni risultanti dalla giurisprudenza che ha interpretato la direttiva 2002/58, può in linea di principio essere giustificato solo

30 Ordinanza di rinvio, punto 46, in fine.

31 Nella sentenza della Corte europea dei diritti dell'uomo (Corte EDU) del 18 gennaio 2022, Adomaitis c. Lituania (CE:ECHR:2022:0118JUD001483318; in prosieguo: la «sentenza della Corte EDU Adomaitis»), che riguardava l'intercettazione di comunicazioni elettroniche dinanzi a un abuso di potere continuato da parte del direttore di un istituto penitenziario, vengono forniti suggerimenti per valutare questa equivalenza.

32 In linea di principio, non si possono equiparare, da un lato, condotte sanzionabili il cui perseguimento avviene mediante il procedimento penale e, dall'altro, illeciti meramente deontologici, la cui sanzione è formalizzata mediante un procedimento disciplinare. Il procedimento penale e quello disciplinare si differenziano, per quanto riguarda l'oggetto, per la natura e la gravità della condotta perseguita. La differenza fra i procedimenti è, in tal senso, indicativa della diversa gravità dei loro rispettivi oggetti.

33 Nella Convenzione istituita sulla base dell'articolo K.3, paragrafo 2, lettera c), del trattato sull'Unione europea, relativa alla lotta contro la corruzione nella quale sono coinvolti funzionari delle Comunità europee o degli Stati membri dell'Unione europea (GU 1997, C 195, pag. 2), sono contemplati casi di corruzione passiva («quando il funzionario deliberatamente, direttamente o tramite un intermediario, sollecita o riceve vantaggi di qualsiasi natura, per sé o per un terzo, o ne accetta la promessa per compiere o per omettere un atto proprio delle sue funzioni o nell'esercizio di queste, in violazione dei suoi doveri di ufficio») e attiva («quando una persona deliberatamente promette o dà, direttamente o tramite un intermediario, un vantaggio di qualsivoglia natura ad un funzionario, per il funzionario stesso o per un terzo, affinché questi compia o ometta un atto proprio delle sue funzioni o nell'esercizio di queste, in modo contrario ai suoi doveri d'ufficio»), che sono da classificare come illeciti penali.

dall'obiettivo di interesse generale per il quale tale conservazione è stata imposta a tali fornitori. La situazione è diversa solo se l'importanza dell'obiettivo perseguito dall'accesso supera quella dell'obiettivo che ha giustificato la conservazione» [34];

– «[i]n particolare, (…) l'accesso ai dati di cui trattasi a fini di repressione e sanzione di un reato comune non può essere accordato in alcun caso qualora la loro conservazione sia stata giustificata dall'obiettivo di lotta alla criminalità grave o, a fortiori, di salvaguardia della sicurezza nazionale» [35].

66. Si applica dunque una sorta di principio di equivalenza tra gli obiettivi di interesse pubblico che giustificano l'*acquisizione* dei dati personali, da un lato, e quelli che legittimano il loro *uso* successivo, dall'altro. L'unica eccezione al suddetto principio è, come sopra esposto, che l'importanza dell'obiettivo perseguito dall'accesso sia maggiore di quella dell'obiettivo che ha giustificato la conservazione.

67. Dare un'interpretazione diversa significherebbe snaturare il sistema di garanzie della direttiva 2002/58: i diritti da essa tutelati potrebbero essere oggetto di gravi ingerenze al di fuori dei casi previsti dall'articolo 15 e delle condizioni stabilite dalla giurisprudenza della Corte di giustizia.

68. In particolare, sacrificare l'integrità del diritto alla riservatezza delle comunicazioni è legittimamente ammissibile solo alla luce dello specifico obiettivo di interesse generale che si persegue. È per questo motivo che la legittimità dell'accesso ai dati conservati deve essere verificata caso per caso, soppesando la gravità che comporta, da un lato, e l'importanza dell'obiettivo di interesse generale che si intende perseguire con tale ingerenza, dall'altro.

69. Non può invece ammettersi un'interpretazione della direttiva 2002/58 secondo cui l'accesso fornito in occasione di una fattispecie iniziale che lo giustifichi validamente apra la strada a un accesso successivo (in realtà, un riutilizzo dei dati ottenuti) basato su un obiettivo gerarchicamente inferiore a quello della fattispecie originaria.

70. A tal fine, i requisiti per l'accesso iniziale (compresi quelli richiesti dalla Corte di giustizia in merito alla sua autorizzazione) [36] sono trasferibili all'uso successivo degli stessi dati da parte di altre autorità.

C. In subordine: incidenza della direttiva 2016/680

71. Finora ho esposto quello che ritengo essere il modo più appropriato di rispondere alla domanda di pronuncia pregiudiziale nei suoi stessi termini, vale a dire, fornendo al giudice del rinvio l'interpretazione della direttiva 2002/58, così come richiesto.

72. Nell'ipotesi in cui i dati controversi in questa causa fossero stati ottenuti non sulla base dell'articolo 15, paragrafo 2, della direttiva 2002/58, bensì direttamente dai servizi di informazione criminale dello Stato membro, nell'ambito di un procedimento penale, lo scenario sarebbe diverso.

[34] Sentenza Commissioner of An Garda Síochána, punto 98.

[35] Sentenza La Quadrature du Net, punto 166.

[36] Sentenza Commissioner of An Garda Síochána, punto 106, che cita la sentenza Prokuratuur, punto 51.

73. In tale ipotesi, entrerebbero in gioco le norme del diritto nazionale, fatta salva l'applicazione della direttiva 2016/680 per quanto riguarda il trattamento dei dati personali ottenuti nel corso di un'indagine penale. Parto dal presupposto che le azioni dei servizi di informazione criminale, in casi come questo, rientrino nell'ambito di applicazione della direttiva 2016/680. Ciò è stato confermato in udienza.

74. Come ho esposto nelle conclusioni presentate nella causa Inspektor v Inspektorata kam Visshia sadeben savet (Finalità del trattamento di dati – Istruttoria penale)[37], «l'RGPD e la direttiva 2016/680 configurano un sistema coerente in cui:

– all'RGPD spetta fissare le *norme generali* per la protezione delle persone fisiche con riguardo al trattamento dei loro dati personali;

– la direttiva 2016/680 detta le *norme specifiche* per il trattamento di tali dati nell'ambito della cooperazione giudiziaria in materia penale e della cooperazione di polizia»[38].

75. Ho poi ricordato[39] che:

– «La tutela fornita dal regime costituito dalle due normative si basa sui principi di liceità, correttezza, trasparenza e, per quanto qui rileva, sul principio della stretta limitazione della raccolta dei dati e del loro trattamento alle finalità previste dalla legge».

– «In particolare, l'articolo 5, paragrafo 1, lettera b), dell'RGPD prevede che i dati siano "raccolti per finalità determinate, esplicite e legittime, *e successivamente trattati in modo che non sia incompatibile con tali finalità*". In questi termini si esprime anche, in quanto *lex specialis*, l'articolo 4, paragrafo 1, lettera b), della direttiva 2016/680».

– «Pertanto, i dati personali non possono essere raccolti né trattati in generale, bensì solo per finalità determinate e alle condizioni di liceità stabilite dal legislatore dell'Unione»[40].

– «Il principio dello stretto collegamento tra la raccolta e il trattamento dei dati, da un lato, e le finalità che le due operazioni devono perseguire, dall'altro, non ha carattere assoluto, in quanto sia l'RGPD che la direttiva 2016/680 consentono una certa flessibilità (...)».

76. Ebbene, secondo l'interpretazione della Corte di giustizia dell'articolo 4, paragrafo 2, della direttiva 2016/680[41], difficilmente si potrà ammettere che i dati personali raccolti nel corso di un procedimento penale siano utilizzati *per la medesima finalità* nell'ambito di un ulteriore procedimento disciplinare nei confronti di un pubblico ufficiale.

37 C-180/21 (EU:C:2022:406); in prosieguo: le «conclusioni Inspektor v Inspektorata».

38 Conclusioni Inspektor v Inspektorata, paragrafo 35.

39 Conclusioni Inspektor v Inspektorata, paragrafi da 36 a 39.

40 Il requisito della «liceità» è richiesto dall'articolo 5, paragrafo 1, lettera a), dell'RGPD [articolo 4, paragrafo 1, lettera a), della direttiva 2016/680], specificando all'articolo 6 dello stesso regolamento quali siano le sue condizioni. Per quanto qui interessa e conformemente alla lettera e) di quest'ultima disposizione, il trattamento deve essere necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare (del trattamento stesso).

41 Sentenza dell'8 dicembre 2022, Inspektor v Inspektorata kam Visshia sadeben savet (Finalità del trattamento dei dati personali – Indagine penale), C-180/21 (EU:C:2022:967); in prosieguo: «sentenza Inspektor v Inspektorata».

77. Devo tuttavia ricordare che, ai sensi dell'articolo 4, paragrafo 2, della direttiva 2016/680, «il trattamento da parte dello stesso o di un altro titolare del trattamento per una qualsiasi delle finalità di cui all'articolo 1, paragrafo 1, diversa da quella per cui sono raccolti i dati personali, è consentito nella misura in cui:

– il titolare del trattamento è autorizzato a trattare tali dati personali per detta finalità conformemente al diritto dell'Unione o dello Stato membro; e

– il trattamento è necessario e proporzionato a tale altra finalità conformemente al diritto dell'Unione o dello Stato membro».

78. Partendo da questa premessa, il giudice del rinvio deve valutare se la (*diversa*) finalità dell'ulteriore trattamento rientri tra quelle previste dall'articolo 1, paragrafo 1, della direttiva 2016/680 o se si trovi al di fuori di queste ultime:

– nel primo caso (riassegnazione ad intra), occorre verificare che siano soddisfatte le due condizioni previste dall'articolo 4, paragrafo 2, della direttiva 2016/680;

– nel secondo caso (riassegnazione ad extra), entra in gioco l'articolo 9, paragrafo 1, della direttiva 2016/680.

1. Uso dei dati ai sensi dell'articolo 4, paragrafo 2, della direttiva 2016/680

79. Per quanto riguarda la *prima* delle due condizioni richieste dalla disposizione, essa sarà soddisfatta solo se il diritto dello Stato membro assume la forma di una legge [42] che disciplina il momento in cui il titolare è autorizzato a trattare i dati personali. Detta legge deve inoltre contenere norme vincolanti, chiare e precise [43].

80. Tuttavia, si tratta ovviamente di una questione che spetta al giudice del rinvio verificare, dopo aver analizzato l'articolo 177 del CPP, l'articolo 19, paragrafo 3, della LIC e le raccomandazioni della procura generale [44]. Sulla base di questi elementi, dovrà valutare in che misura il diritto nazionale consenta che le informazioni ottenute nel corso di un procedimento penale possano essere utilizzate, a determinate condizioni, nell'ambito di indagini su illeciti disciplinari. In questa verifica possono essere utili le considerazioni della sentenza della Corte EDU Adomaitis [45].

81. Per quanto riguarda la *seconda* condizione, il giudice del rinvio dovrà valutare se, nel trattamento dei dati di cui trattasi nella presente causa, l'ingerenza fosse necessaria e proporzionata [46].

[42] Concordo con la Commissione secondo la quale, poiché l'uso successivo dei dati personali ottenuti nel corso di un'indagine penale costituisce un'ingerenza nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta, è ineludibile, ai sensi dell'articolo 52, paragrafo 1, della Carta, che sia previsto per legge.

[43] Paragrafo 51 delle presenti conclusioni.

[44] Nota 12 delle presenti consclusioni.

[45] Sentenza nel cui punto 83 si ritiene sufficiente la garanzia di legittimità dell'ingerenza assicurata dalle disposizioni legislative nazionali e dalla giurisprudenza costituzionale lituana.

[46] Come rilevato dalla Commissione, la presente causa non è molto diversa da quella esaminata nella sentenza della Corte EDU del 16 giugno 2016, Versini-Campinchi e Crasnianski c. Francia (CE:ECHR:2016:0616JUD004917611). Secondo il punto 57 di quest'ultima, risponde a una finalità legittima, conformemente all'articolo 8 della CEDU, l'utilizzo, nell'ambito di un procedimento disciplinare per violazione del segreto professionale, delle comunicazioni avvenute nell'ambito di un procedimento penale. La stretta correlazione sostanziale tra i rispettivi oggetti dei procedimenti penali e disciplinari porta alla comune legittimità degli obiettivi degli uni e degli altri.

82. Ancora una volta, le affermazioni della sentenza della Corte EDU Adomaitis possono contribuire a questa valutazione:

– per quanto riguarda la necessità, occorrerà valutare fino a che punto l'insufficienza probatoria di altri dati disponibili nel corso del procedimento disciplinare abbia reso realmente necessario, per il successo dell'indagine in corso, l'utilizzo dei dati controversi [47];

– per quanto riguarda la proporzionalità, occorre valutare la gravità della violazione che ha dato origine al procedimento disciplinare, tenendo presente che, come sostenuto dal governo lituano e come si evince dalla sentenza della Corte EDU Adomaitis [48], l'uso dei dati personali è riservato ai casi di violazioni per le quali è prevista la sanzione disciplinare più grave, vale a dire la revoca dalle funzioni.

2. Uso dei dati ai sensi dell'articolo 9 della direttiva 2016/680

83. Conformemente all'articolo 9, paragrafo 1, della direttiva 2016/680, i dati personali raccolti dalle autorità competenti per le finalità di cui all'articolo 1, paragrafo 1, possono essere trattati per finalità diverse da quelle di cui all'articolo 1, paragrafo 1, quando tale trattamento è autorizzato dal diritto dell'Unione o dello Stato membro. In tal caso, si applica l'RGPD, a meno che il trattamento non sia effettuato nell'ambito di un'attività che non rientra nell'ambito di applicazione del diritto dell'Unione [49].

84. Nel caso in cui il giudice del rinvio ritenga inapplicabile l'articolo 4, paragrafo 2, della direttiva 2016/680, dovrà ricorrere all'RGPD. Conformemente a tale regolamento, occorrerà chiarire se, oltre alle disposizioni di legge, sia soddisfatta almeno una delle condizioni di liceità del trattamento dei dati personali elencate tassativamente all'articolo 6, paragrafo 1 dello stesso.

V. Conclusione

85. Alla luce di quanto precede, propongo alla Corte di giustizia di rispondere allo Lietuvos vyriausiasis administracinis teismas (Corte amministrativa suprema, Lituania) nei seguenti termini:

«1. L'articolo 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), 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:

[47] Sentenza della Corte EDU Adomaitis, punto 85.

[48] Sentenza della Corte EDU Adomaitis, punto 87.

[49] Questa eccezione è stata interpretata in modo restrittivo nella sentenza del 22 giugno 2021, Latvijas Republikas Saeima (Punti di penalità per infrazioni stradali) (C-439/19, EU:C:2021:504), punto 66.

non consente alle autorità pubbliche competenti di raccogliere i dati conservati dai fornitori di servizi di comunicazione elettronica che possono fornire informazioni dettagliate su un utente e di utilizzarli nell'ambito di indagini per condotte che costituiscono illeciti meno gravi rispetto a quelli oggetto di precedenti indagini che abbiano potuto giustificare l'accesso a detti dati.

2. In subordine:

L'articolo 9, paragrafo 1, della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, in combinato disposto con gli articoli 6 e 10 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, alla luce degli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea,

deve essere interpretato nel senso che:

non osta all'utilizzo, in un procedimento amministrativo disciplinare, di dati personali legittimamente e direttamente acquisiti dall'autorità pubblica nell'ambito di un'indagine penale, a condizione che, in conformità a norme chiare, precise e vincolanti del diritto nazionale, tale procedimento e detta indagine siano collegati e nella misura in cui l'utilizzo dei dati abbia una finalità legittima e sia necessario e proporzionato, circostanza che spetta all'autorità giudiziaria verificare».