Raccolta della giurisprudenza

CONCLUSIONI DELL'AVVOCATO GENERALE
M. CAMPOS SÁNCHEZ-BORDONA
presentate il 20 aprile 2023 [1]

Causa C-548/21

C.G.
contro
Bezirkshauptmannschaft Landeck

[domanda di pronuncia pregiudiziale proposta dal Landesverwaltungsgericht Tirol (Tribunale amministrativo regionale del Tirolo, Austria)]

«Rinvio pregiudiziale – Telecomunicazioni – Protezione dei dati personali – Direttiva (UE) 2016/680 – Procedimento penale –Tentativo di accesso delle autorità pubbliche ai dati registrati in un telefono cellulare senza autorizzazione giudiziaria o di un'entità amministrativa indipendente»

1. La domanda di pronuncia pregiudiziale in esame verte, in sintesi, sulle condizioni che le autorità di polizia devono rispettare per accedere ai dati conservati nel telefono cellulare della persona nei confronti della quale è in corso un'indagine penale.

2. Come cercherò di spiegare, il rinvio pregiudiziale presenta notevoli lacune per quanto riguarda la sua ricevibilità. Qualora la Corte di giustizia decidesse comunque di esaminare il merito, dovrà pronunciarsi sui rispettivi ambiti di applicazione della direttiva 2002/58/CE [2] e della direttiva (UE) 2016/680 [3].

[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).

I. Contesto normativo

A. Diritto dell'Unione

1. Regolamento (UE) 2016/679[4]

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

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

(…)

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».

2. Direttiva 2016/680

4. Il considerando 2 enuncia quanto segue:

«I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei loro dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali (…). La presente direttiva è intesa a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia».

5. Il considerando 46 è così formulato:

«Qualsiasi limitazione dei diritti dell'interessato deve essere conforme alla Carta e alla CEDU, come interpretate nella giurisprudenza rispettivamente della Corte di giustizia e della Corte europea dei diritti dell'uomo [5], e rispettare in particolare la sostanza di tali diritti e libertà».

6. Il considerando 49 così recita:

«Se i dati personali sono trattati nel corso di un'indagine penale e di un procedimento giudiziario penale, gli Stati membri dovrebbero poter prevedere che i diritti di informazione, accesso, rettifica o cancellazione di dati personali e limitazione di trattamento siano esercitati conformemente alle norme nazionali sui procedimenti giudiziari».

7. L'articolo 1 («Oggetto e obiettivi») dispone quanto segue:

«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.

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 In prosieguo: la «Corte EDU».

2. Ai sensi della presente direttiva gli Stati membri:

a) tutelano i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali; e

(…)

3. La presente direttiva non pregiudica la facoltà degli Stati membri di prevedere garanzie più elevate di quelle in essa stabilite per la tutela dei diritti e delle libertà dell'interessato con riguardo al trattamento dei dati personali da parte delle autorità competenti».

8. 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».

9. L'articolo 3 («Definizioni») stabilisce quanto segue:

«Ai fini della presente direttiva si intende per:

(…)

2) "trattamento": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

(…)

7) "autorità competente":

   a) qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; o

(…)».

10. L'articolo 4 («Principi applicabili al trattamento di dati personali»), paragrafo 1, così dispone:

«Gli Stati membri dispongono che i dati personali siano:

a) trattati in modo lecito e corretto;

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

c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati;

(…)

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

f) trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali».

11. L'articolo 8 («Liceità del trattamento») stabilisce quanto segue:

«1. Gli Stati membri dispongono che il trattamento sia lecito solo se e nella misura in cui è necessario per l'esecuzione di un compito di un'autorità competente, per le finalità di cui all'articolo 1, paragrafo 1, e si basa sul diritto dell'Unione o dello Stato membro.

2. Il diritto dello Stato membro che disciplina il trattamento nell'ambito di applicazione della presente direttiva specifica quanto meno gli obiettivi del trattamento, i dati personali da trattare e le finalità del trattamento».

12. L'articolo 13 («Informazioni da rendere disponibili o da fornire all'interessato») così dispone:

«1. Gli Stati membri dispongono che il titolare del trattamento metta a disposizione dell'interessato almeno le seguenti informazioni:

(…)

d) il diritto di proporre reclamo a un'autorità di controllo e i dati di contatto di detta autorità;

(…)

3. Gli Stati membri possono adottare misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato ai sensi del paragrafo 2 nella misura e per il tempo in cui ciò costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di:

a) non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;

b) non compromettere la prevenzione, l'indagine, l'accertamento o il perseguimento di reati o l'esecuzione di sanzioni penali;

c) proteggere la sicurezza pubblica;

d) proteggere la sicurezza nazionale;

e) proteggere i diritti e le libertà altrui.

(…)».

13. Ai sensi dell'articolo 15 («Limitazioni del diritto di accesso»), paragrafo 1:

«Gli Stati membri possono adottare misure legislative volte a limitare, in tutto o in parte, il diritto di accesso dell'interessato nella misura e per il tempo in cui tale limitazione totale o parziale costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di:

a) non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;

b) non compromettere la prevenzione, l'indagine, l'accertamento o il perseguimento di reati o l'esecuzione di sanzioni penali;

c) proteggere la sicurezza pubblica;

d) proteggere la sicurezza nazionale;

e) proteggere i diritti e le libertà altrui».

14. In forza dell'articolo 27 («Valutazione d'impatto sulla protezione dei dati»):

«1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, gli Stati membri dispongono che il titolare del trattamento effettui, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

2. La valutazione di cui al paragrafo 1 contiene almeno una descrizione generale dei trattamenti previsti, una valutazione dei rischi per i diritti e le libertà degli interessati, le misure previste per affrontare tali rischi, le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità alla presente direttiva, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione».

15. L'articolo 28 («Consultazione preventiva dell'autorità di controllo») così recita:

«1. Gli Stati membri dispongono che il titolare del trattamento o il responsabile del trattamento consulti l'autorità di controllo prima del trattamento di dati personali che figureranno in un nuovo archivio di prossima creazione se:

a) una valutazione d'impatto sulla protezione dei dati di cui all'articolo 27 indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio; oppure

b) il tipo di trattamento, in particolare se utilizza tecnologie, procedure o meccanismi nuovi, presenta un rischio elevato per i diritti e le libertà degli interessati.

(…)».

16. L'articolo 54 («Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento») prevede quanto segue:

«Gli Stati membri dispongono che, fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 52, l'interessato abbia il diritto a un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode ai sensi delle disposizioni adottate a norma della presente direttiva siano stati violati a seguito del trattamento dei propri dati personali in violazione di tali disposizioni».

B. Diritto nazionale

17. L'articolo 18 della Strafprozessordnung[6] attribuisce alla polizia giudiziaria funzioni che servono all'amministrazione della giustizia penale (paragrafo 1). Le indagini della polizia giudiziaria sono di competenza delle autorità preposte alla sicurezza (paragrafo 2). Gli organi del servizio di sicurezza pubblica forniscono il servizio esecutivo di polizia giudiziaria, che consiste nell'indagare e perseguire i reati (paragrafo 3).

18. Conformemente all'articolo 99 della StPO, la polizia giudiziaria indaga d'ufficio o sulla base di una denuncia, nel rispetto dei provvedimenti del pubblico ministero e dei giudici (paragrafo 1). Qualora un atto di indagine richieda un provvedimento del pubblico ministero, in caso di pericolo imminente la polizia giudiziaria può esercitare la corrispondente facoltà anche in assenza di tale provvedimento. In tal caso, deve richiedere immediatamente l'autorizzazione (paragrafo 2).

19. Ai sensi dell'articolo 111, paragrafo 2, della StPO, quando le informazioni contenute su supporti per dati devono essere oggetto di una raccolta di dati, chiunque è tenuto a consentire l'accesso a tali informazioni e, su richiesta, a consegnare o consentire la realizzazione di un supporto elettronico di dati in un formato di archiviazione comunemente utilizzato. Inoltre, si deve consentire la realizzazione di una copia di riserva delle informazioni contenute nei supporti per dati.

II. Fatti, controversia e questioni pregiudiziali

20. C.G. è un cittadino tedesco che lavora e risiede in Austria.

21. Il 23 febbraio 2021, durante un controllo sugli stupefacenti, un pacco indirizzato a C.G. e contenente 85 grammi di cannabis in foglie veniva sequestrato dai funzionari dell'ufficio delle dogane di Innsbruck (Austria).

22. Il 6 marzo 2021 due agenti di polizia interrogavano C.G. in merito al mittente del pacco e perquisivano la sua abitazione. Nel corso di questa perquisizione, veniva sequestrato il suo telefono cellulare (che conteneva una scheda SIM e una scheda SD) e consegnato il verbale di sequestro.

23. Alla richiesta di consentire l'accesso ai tabulati telefonici del suo telefono cellulare, C.G. rifiutava, così come rifiutava di rendere noti i codici di accesso al telefono.

[6] Codice di procedura penale. In prosieguo: la «StPO». BGBl n. 631/1975, nella versione applicabile al momento dei fatti (BGBl I n. 24/2020).

24. Il comando di polizia del distretto di Landeck (Austria) non riusciva a sbloccare il telefono cellulare. Esso veniva inviato al Bundeskriminalamt (ufficio federale di polizia giudiziaria) di Vienna (Austria), dove veniva effettuato un nuovo tentativo, non riuscito, di sbloccare il telefono e di leggere i dati in esso contenuti.

25. Nel momento in cui sono state adottate dalla polizia, tali misure non erano disposte né da un provvedimento del pubblico ministero né da una decisione giudiziaria.

26. Il 31 marzo 2021 C.G. presentava reclamo dinanzi al Landesverwaltungsgericht Tirol (Tribunale amministrativo regionale del Tirolo, Austria) contro la misura coercitiva impostagli, impugnando il sequestro del suo telefono cellulare. Quest'ultimo gli veniva restituito il 20 aprile 2021.

27. C.G. non è stato informato dei tentativi di analisi del contenuto del telefono cellulare; ne è venuto a conoscenza perché l'agente di polizia che ha eseguito il sequestro e ha successivamente avviato l'analisi digitale è stato sentito come testimone con l'obbligo di dire la verità. Questo tentativo non è neppure documentato in alcun atto della polizia giudiziaria.

28. In tale contesto, il Landesverwaltungsgericht Tirol (Tribunale amministrativo regionale del Tirolo) ha sottoposto alla Corte di giustizia le seguenti questioni pregiudiziali:

«1) Se l'articolo 15, paragrafo 1 (eventualmente in combinato disposto con l'articolo 5) della direttiva 2002/58, come modificata dalla direttiva 2009/136/CE, letto alla luce degli articoli 7 e 8 della Carta (…), debba essere interpretato nel senso che l'accesso delle autorità pubbliche ai dati conservati nei telefoni cellulari comporta un'ingerenza nei diritti fondamentali sanciti da detti articoli della Carta che presenta una gravità tale che il suddetto accesso deve essere limitato, in materia di prevenzione, ricerca, accertamento e perseguimento dei reati, alla lotta contro la criminalità grave.

2) Se l'articolo 15, paragrafo 1 della direttiva 2002/58, come modificata dalla direttiva 2009/136, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta (…), debba essere interpretato nel senso che osta a una normativa nazionale, quale l'articolo 18 in combinato disposto con l'articolo 99, paragrafo 1, della [StPO], in forza della quale le autorità preposte alla sicurezza si procurano autonomamente, nel corso di un'indagine penale, un accesso completo e non controllato a tutti i dati digitali conservati in un telefono cellulare, senza l'autorizzazione di un giudice o di un'entità amministrativa indipendente.

3) Se l'articolo 47 della Carta, eventualmente in combinato disposto con gli articoli 41 e 52 della Carta (…), sotto il profilo della parità delle armi e sotto il profilo di un mezzo di ricorso effettivo, debba essere inteso nel senso che osta a una normativa di uno Stato membro, quale l'articolo 18 in combinato disposto con l'articolo 99, paragrafo 1, della [StPO], la quale consenta di analizzare digitalmente un telefono cellulare senza che l'interessato ne sia informato preventivamente o, almeno, successivamente all'esecuzione della misura».

III. Procedimento dinanzi alla Corte di giustizia

29. La domanda di pronuncia pregiudiziale è pervenuta alla Corte di giustizia il 6 settembre 2021.

30. Il 20 ottobre 2021 la Corte ha chiesto al giudice del rinvio di dichiarare se la direttiva 2016/680 potesse essere pertinente nel caso di specie.

31. L'11 novembre 2021 il giudice del rinvio ha risposto che la direttiva 2016/680 deve essere applicata nel procedimento principale.

32. Hanno presentato osservazioni scritte i governi tedesco, austriaco, cipriota, danese, estone, francese, ungherese, irlandese, dei Paesi Bassi, norvegese, polacco e svedese, nonché la Commissione europea.

33. All'udienza tenutasi il 16 gennaio 2023 sono comparsi coloro che avevano presentato osservazioni scritte, ad eccezione dei governi tedesco, ungherese e polacco, nonché il governo finlandese. Essi sono stati tutti invitati dalla Corte di giustizia a concentrare le loro argomentazioni sulla direttiva 2016/680 e a rispondere oralmente a determinati quesiti relativi a quest'ultima.

IV. Analisi

A. Irricevibilità

34. Il giudice del rinvio ha inizialmente formulato le sue questioni chiedendo soltanto l'interpretazione della direttiva 2002/58. Tuttavia, quasi tutti gli intervenienti nel procedimento concordano sul fatto che tale direttiva non trova applicazione nella presente causa e che, di conseguenza, la sua interpretazione non è necessaria per risolvere la controversia.

35. Ai sensi del suo articolo 3, la direttiva 2002/58 disciplina il «(…) trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche nell['Unione], comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati».

36. La Corte di giustizia ha dichiarato che, «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]»[7].

37. Nella presente causa, il tentativo di accesso ai dati è stato effettuato direttamente dalle autorità di polizia nell'ambito di un'indagine penale. Non vi è stato alcun intervento dei fornitori di servizi di comunicazioni elettroniche, ai quali non è stato chiesto di comunicare dati personali. La direttiva 2002/58 non è quindi pertinente.

38. La norma del diritto dell'Unione che disciplina la presente fattispecie è la direttiva 2016/680, la quale, conformemente al suo articolo 2, paragrafo 1, si applica al trattamento dei dati personali da parte delle autorità competenti «a fini di (…) indagine (…) di reati».

[7] Sentenza 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») punto 103.

39. Quanto precede sarebbe sufficiente per concludere nel senso dell'irricevibilità del rinvio pregiudiziale, come formulato dal giudice nazionale, poiché la norma del diritto dell'Unione di cui chiedeva l'interpretazione non era applicabile al caso di specie.

40. È vero, tuttavia, che l'articolo 267 TFUE consente alla Corte di giustizia di riformulare le questioni pregiudiziali che le sono sottoposte o di indicare l'esistenza di altre norme del diritto dell'Unione eventualmente pertinenti, al fine di fornire al giudice nazionale una risposta utile [8].

41. La Corte di giustizia si è rivolta al giudice del rinvio affinché si pronunciasse sull'eventuale incidenza della direttiva 2016/680. Essa gli ha quindi offerto la possibilità di integrare o riformulare le sue questioni. Invece di procedere in tal senso, il giudice del rinvio si è limitato a dichiarare che «nella presente causa occorre, in ogni caso, rispettare le disposizioni della direttiva 2016/680», senza tuttavia individuare le disposizioni di detta direttiva sulle quali nutre dubbi né approfondire altre considerazioni nel merito [9].

42. Secondo la giurisprudenza costante della Corte di giustizia, «è indispensabile, come enunciato all'articolo 94, lettera c), del regolamento di procedura, che la decisione di rinvio contenga l'illustrazione dei motivi che hanno indotto il giudice del rinvio a interrogarsi sull'interpretazione o sulla validità di determinate disposizioni del diritto dell'Unione, nonché il collegamento che esso stabilisce tra dette disposizioni e la normativa nazionale applicabile alla causa principale [10]».

43. Da quanto sopra esposto risulta evidente che, nel presente rinvio, sono stati violati i requisiti di cui all'articolo 94 del regolamento di procedura. Anche se la Corte di giustizia dimostra una certa flessibilità al riguardo, la cooperazione con il giudice del rinvio deve essere reciproca: nell'ingiustificata assenza di collaborazione da parte di quest'ultimo nell'esporre i propri dubbi sull'interpretazione del diritto dell'Unione che ritiene applicabile (nella fattispecie, la direttiva 2016/680), mi sembra logico dichiarare irricevibile la domanda di pronuncia pregiudiziale [11].

44. Oltre a quanto sopra, detto giudice:

– non ha specificato la natura del trattamento tentato dalle autorità di polizia, né dei dati personali specificamente cercati. In un primo momento, sembra indicare che si limitasse all'accesso ai dati di connessione (vale a dire i dati sul traffico e sulla localizzazione), ma, in un secondo momento, non esclude che lo sblocco del telefono fosse finalizzato ad accedere a «tutti i dati digitali conservati» [12] e persino al contenuto delle comunicazioni e dei messaggi elettronici scambiati tramite il telefono [13];

– si riferisce sia al sequestro del telefono che all'accesso, o al tentativo di accesso, ai dati in esso contenuti e al loro successivo «utilizzo» (*Auswertung*), vale a dire alla loro analisi e lettura. Quest'ultima, aggiunge, «comporta l'accesso del tutto incontrollato all'intera comunicazione

8 Per tutte, sentenza del 28 aprile 2016, Oniors Bio (C-233/15, EU:C:2016:305), punto 30.

9 La Corte ha ritenuto necessario invitare le parti a indicare «quali siano, a loro avviso, le disposizioni pertinenti della direttiva 2016/680 alla luce delle quali la Corte dovrebbe, se del caso, riformulare le tre questioni pregiudiziali sollevate dal giudice del rinvio» (quarto dei quesiti posti al fine di ottenere una risposta orale in udienza).

10 Sentenza del 6 ottobre 2021, Consorzio Italian Management e Catania Multiservizi (C-561/19, EU:C:2021:799), punto 69.

11 Concordo con il governo francese su questa valutazione (punti da 36 a 41 delle sue osservazioni scritte).

12 In tal senso, nella seconda questione pregiudiziale.

13 Il giudice del rinvio afferma che, «per quanto riguarda i dati di connessione, possono essere ricostruiti quasi tutti i contatti in base alla frequenza, all'orario e alla durata delle comunicazioni; per quanto riguarda le comunicazioni mediante SMS o altri servizi di messaggistica, può essere ricostruito anche il contenuto; anche attraverso l'analisi delle fotografie conservate e delle cronologie del browser viene effettuato un accesso molto intimo nella vita privata dell'interessato».

digitale dell'interessato», il che consente di «ricostruire un quadro molto dettagliato e approfondito di pressoché tutti i settori della vita privata».

45. In tali circostanze, anziché *riformulare* le questioni del giudice a quo, la Corte di giustizia procederebbe a una vera e propria *ricostruzione* del rinvio pregiudiziale, peraltro basata in parte su considerazioni ipotetiche, piuttosto che su fatti accertati. Tutto questo, ripeto, dopo aver dato all'organo giurisdizionale la possibilità di integrare o riformulare le proprie domande.

46. Sono pertanto favorevole a dichiarare irricevibile la domanda di pronuncia pregiudiziale, come richiesto da diversi Stati intervenienti.

47. A questa medesima dichiarazione di irricevibilità si dovrebbe ricondurre la circostanza, sottolineata in udienza, che dinanzi al giudice del rinvio non esiste più una vera controversia che richieda l'interpretazione di norme del diritto dell'Unione.

48. Infatti, il governo austriaco (da cui dipendono le autorità di polizia coinvolte nell'indagine) riconosce che le azioni di tali autorità sono state illecite e hanno violato i diritti della persona interessata. Poiché, secondo l'ordinanza di rinvio, la domanda del ricorrente dinanzi all'organo giurisdizionale amministrativo era diretta, giustamente, contro le misure di polizia che l'amministrazione resistente considera illecite, la controversia sottoposta al giudice del rinvio si è estinta.

49. In ogni caso, laddove la Corte di giustizia non condivida il mio punto di vista, nel prosieguo tratterò, in subordine, i problemi alla base delle questioni pregiudiziali.

50. Prima, tuttavia, ritengo necessario escludere l'esistenza di un altro motivo di irricevibilità dedotto da alcuni degli intervenienti nel procedimento [14]. A loro avviso, poiché la direttiva 2016/680 riguarda la protezione delle persone fisiche con riguardo al *trattamento* dei loro dati, essa non disciplinerebbe casi come quello di cui trattasi, in cui non vi sarebbe stato alcun trattamento, bensì un semplice *tentativo di accesso* a dati che alla fine non è stato possibile ottenere.

51. Secondo la Commissione, invece, l'effetto utile della direttiva 2016/680 dovrebbe privilegiare un'interpretazione del suo oggetto che non si limiti al trattamento dei dati in senso stretto, ma che comprenda anche questioni direttamente collegate ad esso. Una di queste ultime sarebbe il tentativo di accedere ai dati di cui si intende effettuare il trattamento [15].

[14] Mi riferisco, nello specifico, ai governi austriaco, francese, norvegese e dei Paesi Bassi.

[15] Per la Commissione, «è indifferente che i tentativi siano andati o meno a buon fine. Il verificarsi di difficoltà tecniche che impediscono il buon fine dei tentativi di accesso è una circostanza che non può essere conosciuta in anticipo e che non incide sui rischi per la protezione dei dati personali».

52. A mio avviso, senza che sia necessario forzare i limiti dell'ambito di applicazione della direttiva 2016/680 [16], la sua applicazione al caso di specie è giustificata non perché sia avvenuto il sequestro del telefono cellulare [17], bensì per la successiva condotta delle autorità di polizia volta a estrarre da quest'ultimo determinati dati personali dell'interessato, tentando a tal fine di sbloccarlo e di consentire l'accesso al suo contenuto.

53. Tra le operazioni definite come «trattamento» dall'articolo 3, punto 2, della direttiva 2016/680 figura «qualsiasi altra forma di messa a disposizione» dei dati personali, avvenuta nel corso di un'indagine penale. Ritengo che, quando l'autorità di polizia sequestra un telefono in cui sono conservati tali dati e lo manipola per estrarli, avvia una «operazione» di trattamento, anche se questa non va a buon fine per ragioni tecniche attinenti alla sicurezza crittografica.

54. Il tentativo fallito di accesso ai dati personali conservati su un telefono cellulare, nell'ambito di un'indagine penale, è disciplinato dalla direttiva 2016/680 per ragioni analoghe a quelle che hanno indotto la Corte di giustizia a dichiarare applicabile la direttiva 2002/58 al *tentativo* (anch'esso fallito) di ottenere l'autorizzazione giudiziaria per accedere a determinati dati della persona indagata, detenuti da un operatore di comunicazioni elettroniche [18].

55. In tale contesto, se il giudice del rinvio dovesse pronunciarsi sull'illiceità dell'azione di polizia (riconosciuta dal governo austriaco, come ho già esposto), la sua valutazione potrebbe dipendere dalla legittimità dello scopo che con la stessa azione si intende perseguire, indipendentemente dal fatto che la misura sia andata a buon fine o che essa sia stata solo avviata, senza successo.

B. Nel merito

1. Prima questione pregiudiziale

56. Il giudice del rinvio desidera sapere se, ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58 (eventualmente in combinato disposto con l'articolo 5) e alla luce degli articoli 7 e 8 della Carta, «l'accesso delle autorità pubbliche ai dati conservati nei telefoni cellulari comport[i] un'ingerenza nei diritti fondamentali sanciti da detti articoli della Carta che presenta una gravità tale che il suddetto accesso deve essere limitato, in materia di prevenzione, ricerca, accertamento e perseguimento dei reati, alla lotta contro la criminalità grave».

57. Se il rinvio fosse ricevibile, l'inapplicabilità della direttiva 2002/58 imporrebbe di riformulare la prima questione, in modo che la risposta della Corte di giustizia interpreti la direttiva 2016/680.

58. Tale risposta dovrebbe chiarire, in successione, se si possa parlare di ingerenza in casi come quello di specie e, laddove vi sia ingerenza, se la direttiva 2016/680 imponga che l'accesso ai dati sia limitato ai casi di lotta contro la criminalità grave.

[16] In particolare, il ricorso agli articoli 27 e 28 della direttiva 2016/680, suggerito dalla Commissione nelle sue osservazioni scritte, mi sembra superfluo. La «valutazione d'impatto sulla protezione dei dati» di cui all'articolo 27 si riferisce, genericamente, a «un tipo di trattamento» e non a singoli o specifici trattamenti. Ciò emerge dal considerando 58 della direttiva 2016/680: «[l]e valutazioni d'impatto dovrebbero riguardare i sistemi e processi delle operazioni di trattamento pertinenti, *non singoli casi*» (il corsivo è mio). In udienza, la Commissione ha meglio specificato il richiamo alle due disposizioni, che avrebbe citato solo per sottolineare come la direttiva 2016/680 riguardi anche situazioni preliminari al trattamento dei dati propriamente detto.

[17] La direttiva 2016/680 non disciplina il sequestro del telefono in quanto mezzo di prova nell'ambito di un'indagine penale.

[18] Sentenza del 2 ottobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788).

59. Le operazioni di trattamento dei dati possono, per definizione, compromettere i diritti al rispetto della vita privata (articolo 7 della Carta) e alla protezione dei dati personali (articolo 8 della Carta). Le autorità pubbliche devono, pertanto, rispettare le condizioni previste dall'articolo 52, paragrafo 1, della Carta per giustificare la loro interferenza nell'esercizio di tali diritti fondamentali.

60. L'interferenza nei diritti tutelati dagli articoli 7 e 8 della Carta sarà ancora maggiore laddove con la stessa: a) si intenda accedere a dati sensibili abitualmente registrati sui telefoni cellulari e la cui conoscenza può rivelare aspetti della vita dei loro titolari che dovrebbero essere tenuti al riparo dalla conoscenza di terzi; e b) si renda possibile l'accesso al contenuto delle comunicazioni.

61. Orbene, da un punto di vista generale e alla luce del suo contenuto, la direttiva 2016/680 non può essere interpretata nel senso che i trattamenti di dati ai quali si riferisce sono circoscritti ai soli casi di lotta contro la criminalità grave.

62. La direttiva 2016/680 riguarda qualsiasi operazione di trattamento [19] di dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di *tutti i tipi* di reati.

63. Dai principi che la direttiva 2016/680 istituisce in merito al trattamento di dati personali con tali finalità (articolo 4), o dalle condizioni di liceità per effettuarlo (articolo 8), non risulta che, di norma, il trattamento dei dati sia possibile solo nei casi di criminalità grave.

64. Una restrizione limitata ai casi di lotta contro la criminalità grave non potrebbe nemmeno fondarsi semplicemente sull'estrapolazione della giurisprudenza della Corte relativa alla direttiva 2002/58 [20] a casi come quello di specie.

65. A mio avviso, non è possibile farlo perché, fatto salvo quanto argomenterò in seguito, tale giurisprudenza riguarda la conservazione generalizzata e indiscriminata dei dati personali di un gruppo generico e indeterminato, effettuata da fornitori di servizi di comunicazione elettronica con sistematicità. La portata dell'ingerenza che questo genere di conservazione comporta per la società nel suo complesso spiega perché la Corte di giustizia sia stata particolarmente rigorosa nel proibirla e nel prevedere eccezioni a tale divieto.

66. Ciò non si verifica quando l'accesso che si intende eseguire non riguarda la totalità o grandi gruppi della popolazione (vale a dire i dati personali di un gruppo generico e indeterminato), bensì le informazioni contenute in un particolare telefono cellulare, nell'ambito di un procedimento di indagine penale parimenti particolare, per il quale si applica, specificamente, la direttiva 2016/680.

67. La direttiva 2016/680 ha come oggetto soltanto il trattamento di dati da parte delle autorità competenti a fini di prevenzione, indagine accertamento e perseguimento di reati. Tutti i tipi di reati, e non solo quelli gravi.

[19] La tipologia delle «operazioni» di cui all'articolo 3, punto 2, della direttiva 2016/680 è abbastanza ampia. V. la sua trascrizione al paragrafo 9 delle presenti conclusioni.

[20] Sentenze La Quadrature du Net e del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970; in prosieguo: la «sentenza Tele2 Sverige e Watson»); del 2 ottobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788); del 6 ottobre 2020, Privacy International (C-623/17, EU:C:2020:790); e del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche) (C-746/18, EU:C:2021:152; in prosieguo: la «sentenza Prokuratuur»).

68. Inoltre, come sottolineato da alcuni degli intervenienti nel procedimento pregiudiziale, in assenza di qualsiasi indicazione sulla gravità dei reati nella direttiva 2016/680, quest'ultima potrebbe non essere applicata in modo uniforme negli Stati membri, poiché le valutazioni di ciascun ordinamento nazionale in merito alla maggiore o minore gravità di una condotta punibile differiscono notevolmente [21].

69. La direttiva 2016/680, in definitiva, non impone come condizione di liceità che il trattamento di dati personali da essa disciplinato sia possibile solo ai fini della lotta contro la criminalità grave.

70. Quanto precede non osta a che, in applicazione del principio di proporzionalità e caso per caso, il trattamento di dati che le autorità competenti intendono effettuare ai sensi della direttiva 2016/680 sia adeguato sulla base: a) della natura dei reati perseguiti; e b) della qualità dei dati personali cui detto trattamento è indirizzato.

71. In questo senso, concordo con alcune dichiarazioni del governo tedesco sulla limitazione dell'accesso ai dati dei telefoni sequestrati, quando questi permettono, sulla base del loro contenuto digitale, di tracciare un profilo completo della personalità dei loro titolari. Secondo il governo tedesco, tale accesso dovrebbe limitarsi ai dati necessari come mezzo di prova in un caso concreto e potrebbe non essere appropriato in presenza di fattori quali «il carattere minore dell'infrazione oggetto dell'indagine o lo scarso valore probatorio dei dati che si intendono ottenere» [22].

72. In *astratto*, dunque, la direttiva 2016/680 non implica che sia sistematicamente illecito accedere ai dati personali conservati su un telefono cellulare al fine di facilitare le indagini su condotte che possono rientrare nell'ambito della criminalità generale o comune. La valutazione, *nello specifico*, dell'ammissibilità di tale accesso spetterà all'autorità interessata caso per caso, tenendo conto della sua necessità e del criterio di proporzionalità cui ho appena fatto riferimento.

73. Ciò si deduce, a mio avviso, dalle disposizioni della direttiva 2016/680 che stabiliscono le condizioni di validità del trattamento di dati personali nel contesto della lotta contro la criminalità:

– l'articolo 4, paragrafo 1, lettera a), ai sensi del quale i dati devono essere «trattati in modo lecito»;

– l'articolo 8, paragrafo 1, che sottolinea che il trattamento deve essere *necessario* e deve basarsi sul diritto dell'Unione o dello Stato membro.

2. Seconda questione pregiudiziale

74. Con la seconda questione pregiudiziale, il giudice del rinvio desidera sapere se 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, «ost[i] a una normativa nazionale, quale l'articolo 18 in combinato disposto con l'articolo 99, paragrafo 1, della [StPO], in forza della quale le autorità preposte alla

[21] Il governo francese cita come esempio i reati in materia di detenzione e traffico di stupefacenti, sulla cui gravità le norme penali dell'Austria e della Francia differiscono. Il governo svedese si pronuncia in senso analogo.

[22] Osservazioni scritte del governo tedesco, punto 20.

sicurezza si procurano autonomamente, nel corso di un'indagine penale, un accesso completo e non controllato a tutti i dati digitali conservati in un telefono cellulare, senza l'autorizzazione di un giudice o di un'entità amministrativa indipendente».

75. La formulazione della questione presenta una certa ambiguità. Il giudice del rinvio:

– riconosce che l'articolo 110, paragrafo 2, della StPO prevede che le confische dei beni richiedano, in linea di principio, l'autorizzazione del pubblico ministero. L'autorità di polizia può effettuare dette confische, senza autorizzazione, solo nelle ipotesi eccezionali contemplate nel paragrafo 3 del medesimo articolo (che non sembrano verificarsi nel caso in questione);

– aggiunge, tuttavia, che l'analisi delle informazioni conservate sui telefoni cellulari «non è disciplinato in modo univoco [nella StPO]» e potrebbe essere effettuato dalle autorità preposte alla sicurezza di propria iniziativa, senza previa autorizzazione.

76. Il governo austriaco fornisce una versione della normativa nazionale che non è conforme a quella esposta nell'ordinanza di rinvio. In particolare, sostiene che, conformemente al diritto nazionale, sia il sequestro del telefono (salvo i casi di urgenza) sia l'analisi dei dati in esso conservati sono possibili solo con l'autorizzazione del pubblico ministero [23]. Senza un provvedimento del pubblico ministero, l'utilizzo, da parte della polizia, dei dati conservati su quel telefono è illecito.

77. Spetta al giudice del rinvio verificare i termini della normativa nazionale. Nell'ambito del procedimento di cui all'articolo 267 TFUE, la Corte di giustizia non è competente a interpretare il diritto nazionale e spetta unicamente al giudice del rinvio determinare l'esatta portata delle disposizioni legislative, regolamentari e amministrative nazionali [24].

78. Senza voler entrare nella polemica sull'interpretazione del diritto austriaco, mi sembra difficile dedurre dai soli precetti che il giudice del rinvio individua (l'articolo 18 della StPO in combinato disposto con l'articolo 99, paragrafo 1, della medesima legge) le conseguenze che lo stesso trae. Ma, ripeto, si tratta di qualcosa che può decidere solo detto giudice.

79. In ogni caso, il giudice del rinvio ritiene che l'orientamento della sentenza Prokuratuur [25], relativo al controllo preventivo, da parte di un giudice o di un'autorità indipendente, dell'accesso ai dati conservati, possa essere applicabile in una fattispecie come quella in esame.

80. Per il governo dei Paesi Bassi, invece, tale dottrina deve essere intesa nel contesto della normativa nazionale che consentiva alle autorità competenti l'accesso *generale* a *tutti* i dati sul traffico e sull'ubicazione conservati. Ciò spiegherebbe la richiesta di un'autorizzazione giudiziaria preventiva, che tuttavia potrebbe non essere giustificata nel caso dell'accesso ai dati di un singolo telefono cellulare.

[23] Punto 19 delle osservazioni scritte del governo austriaco. Cita la decisione dell'Oberster Gerichtshof (Corte suprema, Austria) del 13 ottobre 2020 (causa 11 Os 56/20z) che qualifica come illecita, in quanto lesivo dei diritti soggettivi dell'interessato, l'analisi da parte della polizia giudiziaria dei dati di un telefono cellulare senza l'autorizzazione del pubblico ministero.

[24] V. per tutte, sentenza del 28 aprile 2022, SeGEC e a., (C-277/21, EU:C:2022:318), punto 21.

[25] Sentenza Prokuratuur, punto 51: «è essenziale che l'accesso delle autorità nazionali competenti ai dati conservati sia subordinato ad un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente, e che la decisione di tale giudice o di tale entità intervenga a seguito di una richiesta motivata delle autorità suddette presentata, in particolare, nell'ambito di procedure di prevenzione o di accertamento di reati ovvero nel contesto di azioni penali esercitate».

81. Su questa stessa linea, il governo norvegese sostiene che tra le numerose garanzie previste dalla direttiva 2016/680 [26] non figura esplicitamente quella della necessità di un'autorizzazione preventiva da parte di un'autorità giudiziaria o amministrativa indipendente.

82. La Commissione, partendo dal presupposto che le disposizioni della direttiva 2016/680 devono essere interpretate alla luce della Carta, sostiene che l'obbligo imposto agli Stati membri dall'articolo 8, paragrafo 1, di tale direttiva (condizioni di liceità del trattamento) comporta la necessità di rispettare i diritti fondamentali garantiti dagli articoli 7 e 8 della Carta.

83. Concordo con la Commissione sul fatto che, pur rispettando detti precetti della Carta, i legislatori nazionali sono tenuti a definire le norme necessarie per garantire che l'accesso ai dati sia giustificato in ciascun caso e limitato a quanto strettamente necessario e proporzionato.

84. Non è tuttavia necessario che tali norme nazionali abbiano come oggetto specifico l'accesso ai dati personali contenuti, come in questo caso, in un telefono cellulare, potendo essere quelle previste dal diritto nazionale in generale in materia di assunzione di prove.

85. A tal riguardo, ho già trascritto il punto 103 della sentenza La Quadrature du Net in merito alle misure degli Stati membri che incidono sulla riservatezza delle comunicazioni elettroniche, senza imporre obblighi di trattamento ai fornitori di detti servizi di comunicazione [27].

86. Senza che sia, pertanto, necessario dedurre dalla direttiva 2016/680 norme *specifiche* di natura procedurale che garantiscano la liceità dell'accesso ai dati conservati su un telefono cellulare [28], si applicheranno le norme nazionali che disciplinano l'esercizio dei poteri di perquisizione e di sequestro nell'ambito delle indagini penali [29].

87. Il rinvio alle disposizioni di diritto interno per garantire la liceità dell'accesso ai sensi della direttiva 2016/680 è, inoltre, in linea con la giurisprudenza della Corte EDU. Proprio in un caso riguardante la Repubblica d'Austria in relazione all'articolo 8 della CEDU (diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza), la Corte EDU ha stabilito che la legge austriaca sul sequestro di oggetti e, in particolare, di documenti, si applica alla perquisizione e al sequestro di dati conservati su supporti informatici [30].

88. Se, come sostiene il governo austriaco, citando la giurisprudenza dell'Oberster Gerichtshof (Corte suprema, Austria), le autorità di polizia non hanno il diritto di accedere ai dati memorizzati su un determinato telefono cellulare senza l'autorizzazione del pubblico ministero, la seconda questione pregiudiziale perde gran parte del suo significato.

[26] Oltre a quelle contenute negli articoli 4 e 8, quelle contenute nei capi III («Diritti dell'interessato»), IV («Titolare del trattamento e responsabile del trattamento»), VI («Autorità di controllo indipendenti») e VIII («Ricorsi, responsabilità e sanzioni»).

[27] V. paragrafo 36 delle presenti conclusioni.

[28] Un'impresa la cui difficoltà è testimoniata dagli sforzi compiuti dalla Commissione ai punti da 34 a 39 delle sue osservazioni per contribuire alla definizione di norme chiare e precise per la definizione dei limiti e delle garanzie adeguate per quanto riguarda l'accesso ai dati di un telefono cellulare.

[29] Norme che, come sottolineano, ad esempio, i governi danese e irlandese, esulano dall'ambito di applicazione del diritto dell'Unione, ma che possono servire a soddisfare un requisito derivante da tale diritto.

[30] Corte EDU, 16 ottobre 2007, Wieser e Bicos Beteiligungen c. Austria (CE:ECHR:2007:1016JUD007433601), § 54: «the Austrian Code of Criminal Procedure does not contain specific provisions for the search and seizure of electronic data. However, it contains detailed provisions for the seizure of objects and, in addition, specific rules for the seizure of documents. It is established in the domestic courts' case-law that these provisions also apply to the search and seizure of electronic data».

89. In ogni caso, la risposta a tale questione non può escludere che l'accesso ai dati personali del telefono sequestrato consenta di «ricostruire un quadro molto dettagliato e approfondito di pressoché tutti i settori della vita privata» dell'interessato [31]. Se così fosse, le autorità di polizia non potrebbero fare a meno dell'autorizzazione preventiva di cui alla sentenza Prokuratuur.

90. A prima vista, questa affermazione sembrerebbe non essere compatibile con la mancata applicazione al caso di specie della direttiva 2002/58 (che interpreta la sentenza Prokuratuur), come ho sostenuto precedentemente. Tuttavia, ritengo che la *ratio* di tale sentenza deponga a favore della stessa soluzione.

91. Nella controversia che ha dato luogo alla sentenza Prokuratuur, sebbene l'accesso sia stato effettuato ottenendo i dati (metadati) presso i fornitori di servizi di comunicazione elettronica, si trattava, come nel presente caso, di un'unica indagine penale, diretta contro una determinata persona. Si trattava della raccolta di «dati relativi a vari numeri di telefono di (…) e diversi codici internazionali di identificazione di apparecchiatura di telefonia mobile di quest'ultima» [32].

92. A mio parere, nella sentenza Prokuratuur, si possono distinguere due livelli: a) quello che mette in discussione la normativa generale di uno Stato membro relativa alla conservazione generalizzata e indifferenziata e all'accesso successivo ai dati detenuti dai fornitori di servizi; e b) quello del controllo preventivo, per un singolo caso, dell'accesso a tali metadati, qualora consentano di delineare un profilo preciso della vita privata di una persona.

93. La circostanza che, nella causa in esame, i dati che rivelano la vita privata non siano detenuti dai fornitori di servizi e siano ottenuti (o si tentino di ottenere) da un unico telefono sequestrato mi sembra di importanza secondaria rispetto alla *ratio* del requisito del controllo preventivo cui si fa riferimento nella sentenza Prokuratuur.

94. Detto controllo preventivo trova il suo fondamento ultimo nella protezione garantita dagli articoli 7 e 8 della Carta. L'autorità che lo effettua deve essere «in grado di garantire un giusto equilibrio tra, da un lato, gli interessi connessi alle necessità dell'indagine nell'ambito della lotta contro la criminalità e, dall'altro, i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali delle persone i cui dati sono interessati dall'accesso» [33].

3. Terza questione pregiudiziale

95. Con la terza questione pregiudiziale, il giudice del rinvio desidera sapere se l'articolo 47 della Carta (eventualmente in combinato disposto con gli articoli 41 e 52 della stessa) osti a una normativa come quella austriaca [34] che «consenta di analizzare digitalmente un telefono cellulare senza che l'interessato ne sia informato preventivamente o, almeno, successivamente all'esecuzione della misura».

96. Ritengo che la questione formulata in questi termini possa risultare superflua per risolvere la controversia, in quanto l'interessato ha potuto esercitare il diritto sancito dall'articolo 47 della Carta chiedendo al giudice del rinvio di dichiarare la nullità dell'azione della polizia sul telefono sequestrato, che comprendeva il successivo (e fallito) utilizzo dei dati in esso conservati.

[31] V. le dichiarazioni del giudice del rinvio trascritte al paragrafo 44 delle presenti conclusioni.

[32] Sentenza Prokuratuur, punto 17.

[33] Sentenza Prokuratuur, punto 52.

[34] Si riferisce nuovamente all'articolo 18 della StPO in combinato disposto con l'articolo 99 della stessa.

97. In merito a questi due momenti dell'azione della polizia, occorre operare una distinzione:

– per quanto riguarda il sequestro del telefono, dalle informazioni del fascicolo risulta che l'interessato ne ha avuto conoscenza e che si è rifiutato di fornire alle autorità di polizia il codice per sbloccarlo quando lo hanno confiscato;

– per quanto riguarda il tentativo di analisi dei dati, tutto lascia intendere che il titolare del trattamento non abbia informato l'interessato di tale operazione, sebbene il governo austriaco dichiari che quest'ultimo era a conoscenza di un rapporto in cui si dava atto dell'azione effettuata sul telefono da parte della polizia giudiziaria [35].

98. Rimangono, dunque, alcune ambiguità circa l'utilizzo dei dati e sulla conoscenza dello stesso da parte dell'interessato che, come ho già sottolineato, il giudice del rinvio avrebbe dovuto chiarire nell'ordinanza di rinvio e che impediscono di dare una risposta utile alla terza questione pregiudiziale.

99. In ogni caso, nel caso in cui la Corte di giustizia non ritenga tale questione irricevibile, mi pronuncerò su di essa. In questa ipotesi, e considerata l'inapplicabilità della direttiva 2002/58, essa andrebbe riformulata alla luce della direttiva 2016/680, i cui articoli 13, 15 e 54 forniscono le indicazioni per rispondere.

100. Ai sensi della direttiva 2016/680, le informazioni relative al trattamento dei suoi dati che devono essere fornite all'interessato sono quelle che risultano necessarie, tra l'altro, per: a) proporre reclamo a un'autorità di controllo [articolo 13, paragrafo 1, lettera d)]; e b) ottenere una tutela giurisdizionale effettiva contro la violazione dei diritti garantiti dalla direttiva 2016/680, fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile (articolo 54).

101. Non va tuttavia dimenticato che sia l'articolo 13, paragrafo 3, sia l'articolo 15, paragrafo 1, della direttiva 2016/680 autorizzano gli Stati membri ad adottare misure legislative intese a:

– ritardare, limitare o escludere la comunicazione di informazioni all'interessato ai sensi del paragrafo 2 dell'articolo 13.

– limitare, in tutto o in parte, il diritto di accesso dell'interessato ai dati trattati, nella misura e per il tempo in cui tale limitazione costituisca una misura necessaria e proporzionata al fine di, *inter alia*, non compromettere indagini o procedimenti ufficiali o giudiziari o pregiudicare l'accertamento di reati [36].

102. In ogni caso, la liceità del trattamento dei dati non dipende dall'adempimento da parte delle autorità competenti degli obblighi (ulteriori) imposti loro dall'articolo 13 della direttiva 2016/680, bensì dalla legittimità della finalità che lo ha giustificato; vale a dire, dal fatto che tali autorità amministrative fossero legittimate ad effettuare il trattamento dei dati personali.

[35] Punto 37 delle sue osservazioni scritte.

[36] V., in tal senso, sentenza Tele2 Sverige e Watson, punto 121. La sua dottrina relativa alla direttiva 2002/58 è trasponibile alla direttiva 2016/680 nel contesto della garanzia della tutela giurisdizionale dei diritti dei titolari di dati oggetto del trattamento.

103. Da questo punto di vista, il fatto che l'interessato sia stato informato dei tentativi di accesso ai dati conservati nel telefono sequestratogli è, di per sé, irrilevante ai fini della liceità per motivi sostanziali dell'azione di polizia. La condotta del titolare del trattamento eventualmente contraria agli obblighi impostigli dall'articolo 13 della direttiva 2016/680 può avere altre conseguenze, ma, ripeto, non pregiudica di per sé la liceità o l'illiceità del trattamento stesso.

104. Spetta al giudice del rinvio stabilire se la normativa nazionale consenta l'esercizio effettivo di tali diritti da parte dell'interessato.

V. Conclusione

105. Alla luce di quanto precede, propongo alla Corte di giustizia di dichiarare irricevibile la domanda di pronuncia pregiudiziale presentata dal Landesverwaltungsgericht Tirol (Tribunale amministrativo regionale del Tirolo, Austria).

In subordine, suggerisco di rispondere a tale domanda nei seguenti termini:

«1) L'articolo 4, paragrafo 1, lettera a), e l'articolo 8, 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, letti alla luce degli articoli 7, 8 e 52, della Carta dei diritti fondamentali dell'Unione europea,

devono essere interpretati nel senso che

nel corso di un'indagine penale, l'accesso delle autorità pubbliche ai dati personali conservati in un telefono cellulare, al fine del loro trattamento, non è limitato ai casi di lotta contro la criminalità grave.

Il suddetto accesso deve essere giustificato in ciascun caso e limitato a quanto strettamente necessario e proporzionato, a seconda della natura dei reati perseguiti e dei dati personali ai quali si intende accedere.

Le autorità di polizia non possono procurarsi, autonomamente e senza l'autorizzazione preventiva di un organo giudiziario, nel corso di un'indagine penale, l'accesso completo e non controllato a tutti i dati conservati in un telefono cellulare, qualora questi consentano di ricavare un profilo preciso della vita privata di una persona.

2) Gli articoli 13, 15 e 54 della direttiva 2016/680, in combinato disposto con gli articoli 47 e 52 della Carta,

devono essere interpretati nel senso che

fatte salve le limitazioni autorizzate dall'articolo 15, paragrafo 1, della direttiva 2016/680 e fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, il titolare di un telefono cellulare deve essere informato del trattamento dei dati personali in esso conservati eventualmente effettuato dalle autorità competenti, nei tempi e nei modi necessari al fine di garantire l'esercizio effettivo del suo diritto a un ricorso giurisdizionale contro l'eventuale violazione dei diritti riconosciuti dalla direttiva 2016/680».