CONCLUSIONI DELL'AVVOCATO GENERALE
ANTHONY MICHAEL COLLINS
presentate l'8 giugno 2023 (1)

Causa C-178/22

Ignoti
con l'intervento di:
Procura della Repubblica presso il Tribunale di Bolzano

[domanda di pronuncia pregiudiziale proposta dal Tribunale di Bolzano (Italia)]

«Rinvio pregiudiziale – Trattamento dei dati personali nel settore delle comunicazioni elettroniche – Riservatezza delle comunicazioni – Fornitori di servizi di comunicazione elettronica – Direttiva 2002/58/CE – Articolo 1, paragrafo 3, e articolo 15, paragrafo 1 – Carta dei diritti fondamentali dell'Unione europea – Articoli 7, 8, 11 e articolo 52, paragrafo 1 – Richiesta del pubblico ministero di accedere ai dati ai fini delle indagini e del perseguimento del furto aggravato di un telefono cellulare – Definizione di "reato grave" idoneo a giustificare una grave ingerenza nei diritti fondamentali – Portata del controllo preventivo diretto a garantire il rispetto del requisito della commissione di un reato grave – Principio di proporzionalità»

I. Introduzione

1. La Procura della Repubblica presso il Tribunale di Bolzano (Italia) (in prosieguo: il «pubblico ministero di Bolzano») chiede al Tribunale di Bolzano (Italia) di autorizzare, ai sensi del diritto nazionale, l'accesso a dati conservati dai fornitori di servizi di comunicazione elettronica che permettano, in particolare, di rintracciare e identificare la fonte e la destinazione di comunicazioni effettuate mediante telefoni cellulari.

2. Nel contesto di tale richiesta, il Tribunale di Bolzano chiede alla Corte di giustizia di interpretare l'articolo 15, paragrafo 1, della direttiva 2002/58/CE (2). Tale disposizione consente agli Stati membri di introdurre eccezioni all'obbligo, enunciato in tale direttiva (3), di garantire la riservatezza delle comunicazioni elettroniche. Nella sentenza nella causa Prokuratuur (4), la Corte ha dichiarato che l'accesso ai dati che consentono di trarre precise conclusioni sulla vita privata di un utente, in applicazione di disposizioni adottate in base all'articolo 15, paragrafo 1, della direttiva 2002/58, costituisce una grave ingerenza nei diritti fondamentali e nei principi sanciti agli articoli 7, 8, 11 e all'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta») (5). Siffatto accesso non può essere autorizzato a fini di prevenzione, ricerca, accertamento e perseguimento di «reati in generale». Esso può essere concesso soltanto nell'ambito di procedure aventi per scopo la lotta contro le «forme gravi di criminalità» (6) e deve essere subordinato a un controllo preventivo effettuato da un giudice o da un'entità amministrativa indipendente al fine di garantire il rispetto di tale requisito (7). Il Tribunale di Bolzano chiede alla Corte di chiarire due aspetti della sentenza Prokuratuur: la nozione di «forme gravi di criminalità» e la portata del controllo preventivo che un giudice deve effettuare sulla base di una disposizione di diritto nazionale che gli impone di autorizzare l'accesso a dati conservati da fornitori di servizi di comunicazione elettronica.

II. Contesto normativo

A. Diritto dell'Unione

3. L'articolo 5 della direttiva 2002/58, intitolato «Riservatezza delle comunicazioni», prevede quanto segue:

«1. 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. (…)

(…)».

4. L'articolo 6 della direttiva 2002/58, intitolato «Dati sul traffico», così dispone:

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

(…)

5. Il trattamento dei dati relativi al traffico ai sensi dei paragrafi da 1 a 4 deve essere limitato alle persone che agiscono sotto l'autorità dei fornitori della rete pubblica di comunicazione elettronica e dei servizi di comunicazione elettronica accessibili al pubblico che si occupano della fatturazione o della gestione del traffico, delle indagini per conto dei clienti, dell'accertamento delle frodi, della commercializzazione dei servizi di comunicazione elettronica o della prestazione di servizi a valore aggiunto. Il trattamento deve essere limitato a quanto è strettamente necessario per lo svolgimento di tali attività.

(…)».

5. L'articolo 9 della direttiva 2002/58, intitolato «Dati relativi all'ubicazione diversi dai dati relativi al traffico», stabilisce quanto segue:

«1. Se i dati relativi all'ubicazione diversi dai dati relativi al traffico, relativi agli utenti o abbonati di reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico possono essere sottoposti a trattamento, essi possono esserlo soltanto a condizione che siano stati resi anonimi o che l'utente o l'abbonato abbiano dato il loro consenso, e sempre nella misura e per la durata necessaria per la fornitura di un servizio a valore aggiunto. Prima di chiedere il loro consenso, il fornitore del servizio deve informare gli utenti e gli abbonati sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti a trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto. Gli utenti e gli abbonati devono avere la possibilità di ritirare il loro consenso al trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico in qualsiasi momento.

(…)».

6. L'articolo 15, paragrafo 1, della direttiva 2002/58 è formulato come segue:

«Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE [(8)], una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea».

B. Diritto nazionale

7. L'articolo 132, comma 3, del decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali (9), come recentemente modificato dall'articolo 1 del decreto-legge 30 settembre 2021 n. 132 - Misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP (10), convertito con modificazioni nella legge 23 novembre 2021 n. 178 (11) (in prosieguo: l'«articolo 132, comma 3, del decreto legislativo n. 196/2003») prevede quanto segue:

«3. Entro il termine di conservazione imposto dalla legge [id est: 24 mesi dalla data della comunicazione], se sussistono sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi, ove rilevanti per l'accertamento dei fatti, i dati sono acquisiti, previa autorizzazione rilasciata dal giudice con decreto motivato, su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altri parti private;

(…)

3-quater: I dati acquisiti in violazione delle disposizioni dei commi 3 e 3-bis non possono essere utilizzati».

8. L'articolo 4 del codice di procedura penale, intitolato «Regole per la determinazione della competenza», così dispone:

«Per determinare la competenza si ha riguardo alla pena stabilita dalla legge per ciascun reato consumato o tentato. Non si tiene conto della continuazione, della recidiva e delle circostanze del reato, fatta eccezione delle circostanze aggravanti per le quali la legge stabilisce una pena di specie diversa da quella ordinaria del reato e di quelle ad effetto speciale».

9. Secondo il giudice del rinvio, il pubblico ministero può perseguire d'ufficio il reato di furto aggravato (12). Ai sensi dell'articolo 625 del codice penale, il colpevole di furto aggravato è punito con una pena ad effetto speciale consistente nella reclusione da due a sei anni e nella multa da EUR 927 a EUR 1 500. L'articolo 624 del codice penale stabilisce che il colpevole di furto semplice, perseguibile a querela della persona offesa, è punito con la reclusione da sei mesi a tre anni e con una multa da EUR 154 a EUR 516.

III. Procedimenti principali e questione pregiudiziale

10. Il pubblico ministero di Bolzano ha avviato due procedimenti penali a carico di ignoti per il furto aggravato di telefoni cellulari, in applicazione degli articoli 624 e 625 del codice penale (13). Al fine di rintracciare i colpevoli, egli ha chiesto al giudice del rinvio, ai sensi dell'articolo 132, comma 3, del decreto legislativo n. 196/2003, «l'autorizzazione ad acquisire presso tutte le compagnie telefoniche tutti i dati in loro possesso, con metodo di tracciamento e localizzazione (in particolare utenze ed eventualmente codici IMEI chiamati/chiamanti, siti visitati/raggiunti, orario e durata della chiamata/connessione ed indicazione delle celle e/o ripetitori interessati, utenze ed IMEI mittenti/destinatari degli SMS o MMS e, ove possibile, generalità dei relativi intestatari) delle conversazioni/comunicazioni telefoniche e connessioni effettuate, anche in roaming, in entrata e in uscita anche se chiamate prive di fatturazione (squilli) dalla data del furto fino alla data di elaborazione della richiesta».

11. Il giudice del rinvio dubita della compatibilità dell'articolo 132, comma 3, del decreto legislativo n. 196/2003 con l'articolo 15, paragrafo 1, della direttiva 2002/58, come interpretato nella sentenza Prokuratuur. Esso osserva che, il 7 settembre 2021, la Corte suprema di cassazione (Italia) (14) ha statuito che, poiché i giudici nazionali dispongono di un margine di discrezionalità nel determinare quali reati costituiscano «forme gravi di criminalità [e] gravi minacce alla sicurezza pubblica», la sentenza Prokuratuur non è direttamente applicabile dai giudici nazionali. A seguito della sentenza della Corte suprema di cassazione, il legislatore italiano ha adottato il decreto legge n. 132, del 30 settembre 2021, il cui articolo 132, comma 3, individua come reati gravi ai fini dell'acquisizione di tabulati telefonici, in particolare, i reati per i quali la legge stabilisce la pena della «reclusione non inferiore nel massimo a tre anni (...)».

12. Secondo il giudice del rinvio, limite edittale di pena previsto all'articolo 132, comma 3, del decreto legislativo n. 196/2003 per la qualificazione di un reato come grave è tale per cui nell'ambito di applicazione di detta norma rientrano reati che destano scarso allarme sociale e che sono puniti soltanto su querela di parte (15). L'accesso ai tabulati telefonici può quindi essere ottenuto, in forza di detta disposizione, in presenza di un furto di un oggetto di valore minimo, come un telefono cellulare o una bicicletta. La soglia prevista all'articolo 132, comma 3, del decreto legislativo n. 196/2003 violerebbe quindi il principio di proporzionalità, alla luce

dell'articolo 52, paragrafo 1, della Carta, il quale impone sempre un bilanciamento tra la gravità del reato oggetto di indagine e la limitazione del godimento di un diritto fondamentale. Il perseguimento di siffatti reati minori non giustifica l'imposizione di limiti al godimento dei diritti fondamentali al rispetto della vita privata, alla protezione dei dati di carattere personale e alla libertà di espressione e di informazione (16).

13. Il giudice del rinvio spiega che i giudici italiani dispongono di un margine discrezionale molto ristretto nel negare l'autorizzazione all'acquisizione dei tabulati telefonici, poiché questa deve essere rilasciata in presenza di «sufficienti indizi di reati» e se siffatta autorizzazione è «rilevant[e] per l'accertamento dei fatti». I giudici, in particolare, non sono competenti a valutare la gravità del reato oggetto dell'indagine. È il legislatore ad aver operato detta valutazione allorché ha stabilito, in termini generali e senza differenziare tra i vari tipi di reato, che l'accesso ai tabulati deve essere concesso, segnatamente, in relazione alle indagini su tutti i reati puniti con la pena della reclusione non inferiore nel massimo a tre anni.

14. In tale contesto, il Tribunale di Bolzano ha deciso di sospendere i procedimenti e di sottoporre alla Corte la seguente questione pregiudiziale:

«Se l'articolo 15, comma 1 della [direttiva 2002/58] osta alla normativa nazionale dell'articolo 132 del [decreto legislativo n. 196/2003], il cui comma 3 (...) così stabilisce:

"3. Entro il termine di conservazione imposto dalla legge, se sussistono sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi, ove rilevanti per l'accertamento dei fatti, i dati sono acquisiti, previa autorizzazione rilasciata dal giudice con decreto motivato, su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altri parti private"».

IV. Procedimento dinanzi alla Corte

15. I governi ceco ed estone, l'Irlanda, i governi francese, italiano, cipriota, ungherese, dei Paesi Bassi, austriaco e polacco, nonché la Commissione europea, hanno presentato osservazioni scritte.

16. Tali parti interessate e il pubblico ministero di Bolzano hanno svolto le loro difese orali e risposto ai quesiti posti dalla Corte nel corso dell'udienza del 21 marzo 2023.

V. Valutazione

A. Ricevibilità

17. Il governo italiano e l'Irlanda sostengono che una parte della domanda di pronuncia pregiudiziale è irricevibile. Sulla base dei fatti esposti dell'ordinanza di rinvio, la richiesta di accesso è stata formulata nel contesto di indagini relative a furti aggravati di telefoni cellulari. L'Irlanda sottolinea che il pubblico ministero può perseguire d'ufficio tali reati. Detta competenza è un riflesso del fatto che la natura e gli effetti del reato colpiscono la società in generale. La domanda di pronuncia pregiudiziale ha quindi carattere ipotetico nella misura in cui riguarda anche reati che possono essere perseguiti soltanto a querela di parte. Il governo italiano rileva che il giudice del rinvio richiama una serie di reati non pertinenti nei procedimenti dinanzi ad esso pendenti. Il governo italiano e la Commissione sostengono che, nonostante il riferimento, nell'ordinanza di rinvio, alla pena della «reclusione non inferiore nel massimo a tre anni», ai sensi dell'articolo 625 del codice penale il reato di furto aggravato è punito con la reclusione da due a sei anni. La Commissione suggerisce pertanto alla Corte di riformulare la questione. Anche il governo francese chiede alla Corte di riformulare la questione. Esso ritiene che, sebbene la Corte possa interpretare disposizioni del diritto dell'Unione, essa non è competente a valutare la compatibilità di norme di diritto interno con la normativa dell'Unione.

18. La questione del giudice del rinvio invita letteralmente la Corte a pronunciarsi sulla compatibilità di una disposizione di diritto nazionale con il diritto dell'Unione. Ciò, di per sé, non impedisce di fornire al giudice del rinvio un'interpretazione del diritto dell'Unione, nel caso di specie dell'articolo 15, paragrafo 1, della direttiva 2002/58, che consentirà a tale giudice di statuire sulla compatibilità di qualsiasi disposizione nazionale oggetto del procedimento di cui è investito (17).

19. Dalla domanda di pronuncia pregiudiziale risulta che il pubblico ministero di Bolzano ha chiesto l'accesso ai dati, segnatamente, per indagare e perseguire due episodi di reato di furto aggravato di telefoni cellulari, in applicazione dell'articolo 625 del codice penale. In tali circostanze, i riferimenti contenuti nell'ordinanza di rinvio ad altri reati, tra cui quelli di cui all'articolo 624 del codice penale (furto semplice) (18), sono irrilevanti ai fini della decisione sulle richieste pendenti dinanzi al giudice del rinvio (19). Nella parte in cui la questione pregiudiziale verte sulla richiesta del pubblico ministero di Bolzano di accedere a dati al fine di indagare sulla commissione di reati di furto aggravato, essa non è ipotetica. Limiterò quindi la mia valutazione dell'applicazione dell'articolo 132, comma 3, del decreto legislativo n. 196/2003 ai fatti descritti dal giudice del rinvio che riguardano i furti aggravati di telefoni cellulari.

B. Merito

1. Osservazioni preliminari

20. La domanda di pronuncia pregiudiziale in esame trae origine da una richiesta del pubblico ministero di Bolzano di accedere a dati conservati da fornitori di servizi di comunicazione elettronica. Essa non riguarda la conservazione di tali dati né la sua liceità ai sensi, in particolare, dell'articolo 15, paragrafo 1, della direttiva 2002/58 (20). I dati consistono in informazioni concernenti le comunicazioni in entrata e in uscita (21) effettuate mediante i telefoni cellulari rubati, nonché in dati relativi all'ubicazione (22). Sebbene i dati non includano il contenuto delle comunicazioni, essi consentono di trarre precise conclusioni sulla vita privata delle persone cui si riferiscono i dati in parola, l'accesso ai quali sembra costituire una «grave» ingerenza nei loro diritti fondamentali (23). L'ingerenza che l'accesso a tali dati comporta può essere giustificata dall'obiettivo (24), indicato all'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58, di prevenzione, ricerca, accertamento e perseguimento di «reati gravi», ma non di reati in generale. Nell'interpretare l'articolo 15, paragrafo 1, della direttiva 2002/58, la Corte opera un collegamento tra la gravità dell'ingerenza nei diritti fondamentali di una persona e la gravità del reato oggetto di indagine (25).

2. Competenza degli Stati membri a definire i «reati gravi»

21. La direttiva 2002/58 disciplina le attività dei fornitori di servizi di comunicazione elettronica in relazione al trattamento dei dati personali (26). L'articolo 1, paragrafo 3, esclude espressamente dall'ambito di applicazione della direttiva 2002/58 le attività dello Stato in determinati settori quali la sicurezza pubblica, la difesa, la sicurezza dello Stato e il diritto penale. Le attività indicate all'articolo 15, paragrafo 1, della direttiva 2002/58 coincidono sostanzialmente con quelle descritte all'articolo 1, paragrafo 3, di quest'ultima e includono attività dello Stato nel settore del diritto penale che sono espressamente escluse dall'ambito di applicazione della direttiva 2002/58 (27). Sussiste quindi un nesso evidente tra le attività dello Stato che l'articolo 1, paragrafo 3, della direttiva 2002/58 esclude dall'ambito di applicazione di tale direttiva e le disposizioni legislative che gli Stati membri possono adottare in forza dell'articolo 15, paragrafo 1, della stessa (28).

22. Nonostante tale chiaro nesso, secondo una giurisprudenza costante della Corte, poiché l'articolo 15, paragrafo 1, della direttiva 2002/58 autorizza espressamente gli Stati membri ad adottare le disposizioni legislative nazionali ivi descritte, siffatte disposizioni rientrano nell'ambito di applicazione della direttiva. Da tale giurisprudenza discende che la nozione di «attività», comprese le «attività dello Stato in settori che rientrano nel diritto penale» di cui all'articolo 1, paragrafo 3, della direttiva 2002/58, non comprende le disposizioni legislative menzionate all'articolo 15, paragrafo 1, di quest'ultima (29).

23. Né l'articolo 2 della direttiva 2002/58, che contiene una serie di definizioni ai fini dell'applicazione di tale direttiva, né altre disposizioni della direttiva 2002/58, ivi compreso l'articolo 15, paragrafo 1, definiscono il termine «reati». La direttiva 2002/58 non contiene un elenco di «reati» (30). Inoltre, la giurisprudenza in materia di interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58 non definisce tale nozione (31).

24. Nonostante l'assenza di siffatte definizioni, la direttiva 2002/58 non stabilisce che ogni Stato membro debba definire i «reati» conformemente al proprio diritto nazionale (32). Secondo una giurisprudenza costante della Corte, in forza di quanto imposto tanto dall'applicazione uniforme del diritto dell'Unione quanto dal principio d'uguaglianza discende che una disposizione di diritto dell'Unione che non contenga alcun espresso richiamo al diritto degli Stati membri per quanto riguarda la determinazione del suo senso e della sua portata dà normalmente luogo, nell'intera Unione, ad un'interpretazione autonoma ed uniforme. Nel contesto dell'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58, il termine «reati» potrebbe, almeno in linea di principio, essere considerato come una nozione autonoma di diritto dell'Unione, che deve essere interpretata in modo uniforme nel territorio di tutti gli Stati membri (33).

25. I 10 Stati membri che hanno presentato osservazioni alla Corte e la Commissione sono tuttavia unanimemente concordi nel ritenere che spetti a ciascuno Stato membro definire i «reati», ivi compresi i reati gravi, richiamati all'articolo 15, paragrafo 1, della direttiva 2002/58 mediante rinvio al diritto nazionale.

26. Condivido tali argomenti per le ragioni esposte nel prosieguo.

27. In primo luogo, la Corte ha già precisato che, nel contesto dell'articolo 15, paragrafo 1, della direttiva 2002/58, spetta agli Stati membri definire gli interessi essenziali della propria sicurezza e decidere le misure idonee a garantire la loro sicurezza interna ed esterna (34). Sebbene non l'abbia espressamente dichiarato, la Corte sembra quindi aver ritenuto che l'espressione «sicurezza nazionale» di cui all'articolo 15, paragrafo 1, della direttiva 2002/58 non sia una nozione autonoma di diritto dell'Unione, nonostante l'assenza di definizione di tale espressione o di un rinvio espresso al diritto degli Stati membri (35). Non vedo alcun motivo per cui questo stesso approccio non debba applicarsi al potere degli Stati membri di definire i «reati» o i «reati gravi» ai fini dell'articolo 15, paragrafo 1, della direttiva 2002/58. I termini «reati», «sicurezza pubblica» e «sicurezza nazionale» contenuti in tale disposizione possono essere considerati *noscitur a sociis*, poiché risulta che il legislatore dell'Unione ha inteso trattare ciascuno di essi in modo analogo, anche per quanto riguarda il modo in cui sono definiti (36).

28. In secondo luogo, l'articolo 4, paragrafo 2, TUE impone all'Unione di rispettare l'identità nazionale degli Stati membri insita nella loro struttura fondamentale, politica e costituzionale. Inoltre, nel preambolo della Carta si riconosce che, mentre l'Unione contribuisce alla salvaguardia e allo sviluppo di valori comuni, essa rispetta la diversità delle culture e delle tradizioni dei popoli d'Europa. La definizione dei reati e delle sanzioni (37) riflette le sensibilità e le tradizioni nazionali, che variano notevolmente non soltanto da uno Stato membro all'altro, ma anche nel corso tempo, parallelamente rispetto alle trasformazioni della società (38).

29. In tale contesto si può osservare che, nella definizione dei reati e delle sanzioni, gli Stati membri tengono conto, in misura variabile, di una gamma di diversi fattori. La valutazione, da parte di uno Stato membro, della «gravità» di un determinato reato si riflette spesso, se non immancabilmente, nella gravità della sanzione prevista. La durata di una pena detentiva può riflettere l'analisi di una serie di fattori, tra i quali la «gravità» intrinseca percepita di un reato e la sua «gravità» relativa rispetto ad altri reati. Non è stato addotto alcun motivo per cui gli Stati membri dovrebbero astenersi dall'esercitare siffatta competenza o, di fatto, perché dovrebbe trovare applicazione un approccio diverso alla definizione di «reati», di «reati gravi» o di «reati in generale» nel contesto specifico di cui trattasi.

30. La competenza degli Stati membri nel settore del diritto penale lascia impregiudicata la competenza di cui gode l'Unione nello stabilire, in determinati casi, ad esempio, norme minime che definiscono reati e sanzioni in relazione alla criminalità particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni (39). Il legislatore dell'Unione non ha tuttavia stabilito norme relative alla definizione dei reati di cui all'articolo 15, paragrafo 1, della direttiva 2002/58 (40). Infatti, come indicato in precedenza (41), dalla formulazione dell'articolo 1, paragrafo 3, della direttiva 2002/58 risulta che, nell'adottare tale direttiva, il legislatore dell'Unione non ha inteso esercitare alcuna competenza in materia penale.

31. Queste due ragioni sono sufficienti a spiegare il motivo per cui, nonostante il fatto che le disposizioni legislative nazionali adottate in forza dell'articolo 15, paragrafo 1, della direttiva 2002/58 ai fini della ricerca e del perseguimento dei reati rientrino nell'ambito di applicazione di tale strumento, gli Stati membri restano competenti a definire i «reati», ivi compresi i «reati gravi», e a determinare le sanzioni applicabili alle relative condotte (42).

3. Livello di controllo dell'esercizio della facoltà di cui all'articolo 15, paragrafo 1, della direttiva 2002/58 di derogare al principio di riservatezza

32. La Corte ha sottolineato che la facoltà di derogare (43), segnatamente, al principio di riservatezza sancito all'articolo 5, paragrafo 1, della direttiva 2002/58, deve essere interpretata in maniera restrittiva, affinché essa non divenga la regola generale, privando così detto principio della sua portata (44). L'esercizio di detta facoltà deve quindi rispettare, in particolare, i principi di equivalenza (45) e di effettività (46). Esso deve altresì rispettare i principi generali del diritto dell'Unione, ivi compreso il principio di proporzionalità (47), nonché gli articoli 7, 8, 11 (48) e l'articolo 52, paragrafo 1, della Carta (49). L'obiettivo della lotta contro la criminalità grave deve sempre essere conciliato con il godimento dei diritti fondamentali in tal modo pregiudicati. I diritti sanciti dagli articoli 7, 8 e 11 della Carta non appaiono come prerogative assolute, e il loro esercizio va considerato alla luce della loro funzione sociale (50). L'articolo 52, paragrafo 1, della Carta stabilisce quindi che le limitazioni all'esercizio di tali diritti, quali previste dalla legge, devono rispettare il contenuto essenziale di detti diritti e, nel rispetto del principio di proporzionalità, essere necessarie e rispondere effettivamente a finalità di interesse generale riconosciute

dall'Unione europea o all'esigenza di proteggere i diritti e le libertà altrui. Le disposizioni legislative nazionali adottate in applicazione dell'articolo 15, paragrafo 1, della direttiva 2002/58 devono quindi rispondere effettivamente e rigorosamente a uno degli obiettivi enunciati in tale disposizione. Esse devono essere fondate su criteri oggettivi, essere giuridicamente vincolanti e prevedere norme chiare e precise che indichino le condizioni sostanziali e procedurali alle quali i fornitori di servizi di comunicazione elettronica devono concedere alle autorità nazionali competenti l'accesso ai dati (51).

33. Al fine di garantire, in pratica, il pieno rispetto di tali condizioni, l'accesso delle autorità nazionali competenti ai dati conservati deve essere subordinato, in linea di principio (52), ad un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente (53), a seguito di una richiesta motivata delle autorità suddette e dell'informazione delle persone interessate (54). Secondo una costante giurisprudenza, nell'effettuare detto controllo preventivo il giudice o l'entità amministrativa indipendente deve conciliare i diversi interessi e diritti in gioco, al fine di garantire un giusto equilibrio tra le necessità dell'indagine e della salvaguardia dei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali degli interessati (55).

34. Nel caso di specie, l'articolo 132, comma 3, del decreto legislativo n. 196/2003 fissa le condizioni alle quali il giudice nazionale deve ingiungere ai fornitori di servizi di comunicazione elettronica di concedere al pubblico ministero, su richiesta di quest'ultimo, l'accesso ai dati. È pacifico (56) che l'articolo 132, comma 3, del decreto legislativo n. 196/2003 enuncia in modo chiaro e preciso le circostanze e le condizioni alle quali un giudice nazionale può ingiungere ai fornitori di servizi di comunicazione elettronica di fornire siffatto accesso. Il giudice del rinvio ritiene, tuttavia, che la pena della «reclusione non inferiore nel massimo a tre anni» sia di portata eccessiva, poiché riconduce nell'ambito di applicazione della disposizione in parola reati, quali il furto semplice, che destano scarso allarme sociale.

35. Sebbene l'articolo 132, comma 3, del decreto legislativo n. 196/2003 riguardi, potenzialmente, un'ampia gamma di reati, la Corte non dispone, nell'ambito del presente procedimento, di alcun elemento idoneo a dimostrare che in esso ricada un numero talmente elevato di reati da rendere l'accesso ai dati ai sensi di tale disposizione la regola anziché l'eccezione (57). La soglia della reclusione non inferiore nel massimo a tre anni, di cui a detta disposizione, non appare eccessivamente bassa (58). Per analogia, l'articolo 3, punto 9, della direttiva 2016/681 (59) definisce i «reati gravi» come i «reati elencati nell'allegato II, che siano punibili con una pena detentiva o una misura di sicurezza privativa della libertà personale non inferiore a tre anni conformemente al diritto nazionale di uno Stato membro» (60). La Corte ha tuttavia dichiarato che, nella misura in cui l'articolo 3, punto 9, della direttiva 2016/681 fa riferimento alla pena massima applicabile, e non alla pena minima, non è escluso che i «dati [di cui trattasi] possano essere oggetto di un trattamento a fini di lotta contro reati che, pur soddisfacendo il criterio previsto da tale disposizione relativo alla soglia di gravità, rientrino, tenuto conto delle peculiarità del sistema penale nazionale, non nei reati gravi, bensì nei reati comuni» (61).

36. La pena di tre anni di cui all'articolo 132, comma 3, del decreto legislativo n. 196/2003 si riferisce alla pena massima applicabile e potrebbe quindi applicarsi a reati quali il furto semplice (62). Occorre quindi esaminare in che modo l'articolo 132, comma 3, del decreto legislativo n. 196/2003 è applicato nella pratica. Fatta salva la verifica del giudice del rinvio, l'articolo 132, comma 3, del decreto legislativo n. 196/2003 pare stabilire due diversi livelli di controllo preventivo da parte del giudice nazionale, a seconda della natura dei reati oggetto di indagine.

37. Il primo di questi livelli di controllo impone (63) ai giudici nazionali di autorizzare il pubblico ministero ad accedere ai dati conservati dai fornitori di servizi di comunicazione elettronica qualora siffatti dati siano rilevanti per l'accertamento dei fatti e sussistano sufficienti indizi della commissione di un reato di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi. Il giudice nazionale deve quindi procedere a una valutazione individuale della gravità del reato di cui si tratti e verificare se l'indagine e il perseguimento di tale reato giustifichino una limitazione dei diritti generali sanciti agli articoli 7, 8 e 11 della Carta, nonché dei diritti specifici contenuti negli articoli 5, 6 e 9 della direttiva 2002/58. Detto livello esige una valutazione individuale, nel caso concreto, della questione se l'ingerenza in siffatti diritti sia proporzionata rispetto all'obiettivo di interesse generale della lotta contro la criminalità.

38. Di converso, il secondo livello di controllo, pertinente nell'ambito del presente procedimento, impone (64) ai giudici nazionali di autorizzare il pubblico ministero ad accedere ai dati conservati dai fornitori di servizi di comunicazione elettronica qualora siffatti dati siano rilevanti per l'accertamento dei fatti e sussistano sufficienti indizi della commissione di reati puniti, segnatamente, con la pena della reclusione non inferiore nel massimo a tre anni. In tal caso, il ruolo del giudice nazionale si limita alla verifica del fatto che tali requisiti oggettivi ricorrano, senza alcuna possibilità di effettuare una valutazione individuale degli interessi in gioco (65). Il controllo effettuato

dal giudice nazionale ai sensi dell'articolo 132, comma 3, del decreto legislativo n. 196/2003 è quindi svincolato da qualsiasi collegamento effettivo con le circostanze specifiche della causa di cui è investito.

39. Sebbene i giudici nazionali possano non essere competenti a sindacare la definizione dei reati da parte del legislatore o la decisione di quest'ultimo quanto alla gravità degli stessi (66), detti giudici devono tuttavia essere competenti a effettuare una valutazione individuale della questione se la concessione dell'accesso, in applicazione di disposizioni legislative adottate in base all'articolo 15, paragrafo 1, della direttiva 2002/58, a dati sensibili che consentono di trarre precise conclusioni sulla vita privata di un utente, accesso che, quindi, costituisce una grave ingerenza nei diritti fondamentali sanciti agli articoli 7, 8, 11 e all'articolo 52, paragrafo 1, della Carta, sia proporzionata.

40. Ne consegue che, ai sensi delle disposizioni adottate sulla base dell'articolo 15, paragrafo 1, della direttiva 2002/58 l'accesso a dati sensibili non può essere concesso salvo che i) il reato di cui trattasi raggiunga la soglia di gravità previamente determinata dal legislatore nazionale e ii) un giudice o un'altra entità amministrativa indipendente stabilisca, a seguito di una valutazione o controllo individuali, che l'ingerenza nei diritti fondamentali determinata dalla concessione di detto accesso sia proporzionata, alla luce dell'obiettivo di interesse generale della lotta contro la criminalità in un caso concreto. In taluni casi, tuttavia, l'accesso a siffatti dati può essere negato anche qualora il reato raggiunga la soglia di gravità prevista dal diritto nazionale.

41. Il reato di furto aggravato di cui al presente procedimento è considerato «grave» ai sensi del diritto nazionale poiché è punibile, segnatamente, con la pena della reclusione da due a sei anni, nel rispetto, dunque, della soglia di gravità prevista all'articolo 132, comma 3, del decreto legislativo n. 196/2003 (67). Non risulta che, nell'applicazione di disposizioni adottate in base all'articolo 15, paragrafo 1, della direttiva 2002/58, i giudici italiani siano competenti a rimettere in discussione la qualificazione del furto aggravato come «reato grave» ai sensi del diritto nazionale. Qualora la soglia fissata dal diritto nazionale non sia raggiunta, il giudice del rinvio non può pertanto concedere l'accesso ai dati richiesti (68).

42. Qualora la soglia fissata dal legislatore nazionale sia raggiunta, il giudice del rinvio deve, in applicazione dell'articolo 15, paragrafo 1, della direttiva 2002/58, controllare se, alla luce di tutte le circostanze che caratterizzano lo specifico caso di cui trattasi, l'ingerenza nei diritti fondamentali determinata dalla concessione dell'accesso a dati sensibili sia proporzionata all'obiettivo di interesse generale della lotta contro tale reato. Il giudice del rinvio deve, a detto riguardo, tenere conto e ponderare tutti i diritti e gli interessi pertinenti, compresi, segnatamente, i danni causati ai diritti di proprietà delle vittime tutelati dall'articolo 17 della Carta, nonché il fatto che i telefoni cellulari possono contenere informazioni altamente sensibili relative alla vita privata, professionale e finanziaria dei loro proprietari (69). L'accesso ai dati in parola può essere l'unico mezzo efficace disponibile per indagare e perseguire i reati di cui trattasi e per garantire che i loro autori, al momento ignoti, non restino impuniti. Anche i diritti dei terzi (70) devono essere presi in considerazione.

43. Per quanto riguarda i diritti dei terzi, dal fascicolo del giudice del rinvio risulta (71) che il pubblico ministero di Bolzano ha chiesto l'accesso ai dati relativi alle comunicazioni effettuate con i telefoni cellulari rubati dal 29 ottobre 2021, per quanto concerne il primo furto commesso il 27 ottobre 2021 (72) e dal 20 novembre 2021, per quanto concerne il secondo furto, commesso in tale data (73). Queste date mostrano che le richieste di accesso incidono, in misura molto limitata, sui diritti delle vittime garantiti, in particolare, dagli articoli 7, 8 e 11 della Carta (74). Il governo italiano ha altresì indicato, nelle sue osservazioni scritte, che il procedimento nazionale verte unicamente su dati utili per individuare l'autore o gli autori dei furti di cui trattasi. Nel caso in cui siano individuate chiamate verso terzi o provenienti da terzi non connesse al furto, tali dati sarebbero distrutti, conformemente all'articolo 269 del codice di procedura penale (75). Infine, l'articolo 132, comma 3-quater, del decreto legislativo n. 196/2003 prevede che i dati acquisiti in violazione delle disposizioni di cui ai commi 3 e 3-bis non possono essere utilizzati (76).

VI. Conclusione

44. Alla luce delle considerazioni che precedono, suggerisco alla Corte di rispondere alla questione pregiudiziale sottoposta dal Tribunale di Bolzano (Italia) nei seguenti termini:

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), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, nonché gli articoli 7, 8, 11 e l'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea

devono essere interpretati nel senso che essi non ostano a una normativa nazionale che impone al giudice di autorizzare il pubblico ministero ad accedere a dati legittimamente conservati dai fornitori di servizi di comunicazione elettronica e che consentono di trarre precise conclusioni sulla vita privata di un utente, qualora tali dati siano rilevanti per l'accertamento dei fatti e sussistano sufficienti indizi della commissione di un reato grave, come definito dal diritto nazionale, punito con la pena della reclusione non inferiore nel massimo a tre anni. Prima di concedere l'accesso, il giudice nazionale deve effettuare una valutazione individuale della questione se l'ingerenza nei diritti fondamentali determinata dalla concessione di siffatto accesso sia proporzionata, alla luce, segnatamente, della gravità del reato in discussione e dei fatti del caso di cui trattasi.

---

1 Lingua originale: l'inglese.

---

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), quale modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009 (GU 2009, L 337, pag. 11).

---

3 V. articolo 5 della direttiva 2002/58. La tutela della riservatezza delle comunicazioni elettroniche, garantita dall'articolo 5, paragrafo 1, della direttiva 2002/58, si applica alle misure adottate da tutti i soggetti diversi dagli utenti, indipendentemente dal fatto che si tratti di soggetti privati o pubblici. Sentenza del 2 ottobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, punto 36 e giurisprudenza ivi citata).

---

4 Sentenza 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»).

---

5 Indipendentemente dalla durata del periodo per il quale l'accesso ai dati suddetti viene richiesto, nonché dalla quantità o dalla natura dei dati disponibili per tale periodo.

---

6 O la prevenzione di gravi minacce alla sicurezza pubblica. V. sentenza Prokuratuur, punti 35, 39 e 45. V. anche sentenze del 2 ottobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, punto 56) e del 6 ottobre 2020, La Quadrature du Net e a. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 140).

---

7 Sentenza Prokuratuur, punti da 48 a 52.

---

8 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).

---

9 Supplemento ordinario alla GURI n. 174 del 29 luglio 2003.

---

10 GURI n. 234 del 30 settembre 2021.

---

11 GURI n. 284 del 29 novembre 2021.

---

12 Il diritto italiano qualifica come «aggravati» i furti oggetto dell'indagine in cui interviene il giudice del rinvio.

---

13 Il primo furto è stato commesso il 27 ottobre 2021 (numero di registro RGNR 9228/2021). Il secondo è avvenuto il 20 novembre 2021 (numero di registro RGNR 9794/2021). I furti dei telefoni cellulari sono stati commessi a Bolzano e sono stati denunciati ai Carabinieri dai rispettivi proprietari.

---

14 Cass. Pen. Sez. II, n. 33116, ud. 7.9.2021, est. Pellegrino.

---

15 Secondo il giudice del rinvio, questo «[è], ad esempio, il caso del reato di violazione del domicilio, punito dall'articolo 614 [del codice penale] con una pena di reclusione da uno a quattro anni. Altri reati, il cui limite di pena edittale non osta all'acquisizione dei tabulati telefonici, puniti su semplice querela di parte poiché di scarso allarme sociale, sono i reati di cui all'articolo 633 [del codice penale] (invasione di terreni e edifici: reclusione da uno a tre anni e multa da Euro 103 a Euro 1.032) o all'articolo 640 [del codice penale] (truffa semplice: reclusione da sei mesi a tre anni e multa da Euro 51 a Euro 1.032)».

---

16 V. articoli 7, 8 e 11 della Carta.

---

17 V., per analogia, sentenza del 17 marzo 2021, Consulmarketing (C-652/19, EU:C:2021:208, punto 33). Secondo una costante giurisprudenza, spetta alla Corte, ai sensi dell'articolo 267 TFUE, fornire al giudice nazionale una risposta che gli consenta di dirimere la controversia sottopostagli. In tale prospettiva, spetta alla Corte, se necessario, riformulare le questioni che le sono sottoposte. Sentenza del 25 luglio 2018, Dyson (C-632/16, EU:C:2018:599, punto 47 e giurisprudenza ivi citata).

---

18 Chiunque commetta il reato di furto semplice è punito con la reclusione da sei mesi a tre anni e, quindi, rientra nell'ambito di applicazione dell'articolo 132, comma 3, del decreto legislativo n. 196/2003.

---

19 Nella parte in cui tali riferimenti indicano che l'articolo 132, comma 3, del decreto legislativo n. 196/2003 può trovare applicazione nell'ambito di indagini su reati non gravi, v. paragrafi da 35 a 39 delle presenti conclusioni.

---

20 La domanda di pronuncia pregiudiziale si basa quindi sulla premessa secondo cui la conservazione dei dati richiesti è lecita. La conservazione e l'accesso a dati cui si applica la direttiva 2002/58 costituiscono ingerenze distinte nei diritti fondamentali garantiti agli articoli 7, 8 e 11 della Carta e richiedono una giustificazione distinta, ai sensi dell'articolo 52, paragrafo 1, della stessa. V., in tal senso, sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a. (C-140/20, EU:C:2022:258, punto 47). I punti da 29 a 33 della sentenza Prokuratuur forniscono una rassegna delle norme che disciplinano la conservazione di tali dati.

---

21 L'articolo 2, lettera d), della direttiva 2002/58 stabilisce che per «comunicazione» si intende «ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico (...)».

---

22 Ai sensi dell'articolo 2, lettera c), della direttiva 2002/58, per «dati relativi all'ubicazione» si intende ogni dato «che indichi la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico».

---

23 Sentenza Prokuratuur, punti 34 e 35. V., per analogia, sentenza del 2 ottobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, punti da 59 a 62). Spetta al giudice nazionale valutare se l'accesso ai dati di cui trattasi costituisca una «grave» ingerenza nei diritti fondamentali delle persone interessate da tali dati. Le presenti conclusioni si basano sulla premessa secondo cui l'ingerenza determinata dall'accesso ai dati descritti al precedente paragrafo 10 è grave.

---

24 L'elenco degli obiettivi di cui all'articolo 15, paragrafo 1, della direttiva 2002/58 ha carattere esaustivo. Sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970, punto 90).

---

25 V., in tal senso, conclusioni dell'avvocato generale Saugmandsgaard Øe nella causa Ministerio Fiscal (C-207/16, EU:C:2018:300, paragrafi da 79 a 82 e giurisprudenza ivi citata). In relazione all'obiettivo della lotta alla criminalità, l'accesso può, in linea di principio, essere consentito, soltanto per i dati di persone sospettate di progettare, di

commettere o di aver commesso un reato grave, o anche di essere implicate in una maniera o in un'altra in un illecito del genere. Sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a. (C-140/20, EU:C:2022:258, punto 105).

---

26 V., in tal senso, l'articolo 3 della direttiva 2002/58, ai sensi del quale quest'ultima si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico. V. anche sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970, punti 70 e 74) e, per analogia, conclusioni dell'avvocato generale Szpunar nella causa La Quadrature du Net e a. (Dati personali e lotta alla contraffazione) (C-470/21, EU:C:2022:838, paragrafo 38).

---

27 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, punto 97).

---

28 Ai fini della salvaguardia della sicurezza nazionale, della difesa, della sicurezza pubblica, della prevenzione, ricerca, accertamento e perseguimento dei reati e dell'uso non autorizzato del sistema di comunicazione elettronica.

---

29 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, punto 98), e del 6 ottobre 2020, Privacy International (C-623/17, EU:C:2020:790, punto 38 e giurisprudenza ivi citata).

---

30 V., di converso, articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri (GU 2002, L 190, pag. 1), come modificata dalla decisione quadro 2009/299/GAI del Consiglio, del 26 febbraio 2002, (GU 2009, L 81, pag. 24) il quale elenca i reati che danno luogo a consegna in base a un mandato d'arresto europeo, nonché l'allegato II della direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi (GU 2016, L 119, pag. 132), il quale contiene un elenco dei «reati gravi» definiti all'articolo 3, punto 9, di tale direttiva.

---

31 La direttiva 2002/58 non contiene alcun riferimento a «reati generali», «reati gravi» o «criminalità». La Corte utilizza tali termini nella sua giurisprudenza senza definirli e senza fornire alcun criterio quanto al modo in cui i legislatori nazionali potrebbero farlo. V., ad esempio, sentenze del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970, punti 115 e 125) e del 2 ottobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:78, punti 54, 56 e 63). V. anche, a tal riguardo, il punto 45 della sentenza Prokuratuur.

---

32 V., di converso, l'articolo 1, paragrafo 1, della direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58 (GU 2006, L 105, pag. 54) ai sensi del quale «[l]a presente direttiva ha l'obiettivo di armonizzare le disposizioni degli Stati membri relative agli obblighi, per i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione, relativi alla conservazione di determinati dati da essi generati o trattati, allo scopo di garantirne la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi, *quali definiti da ciascuno Stato membro nella propria legislazione nazionale*» (il corsivo è mio). Con sentenza dell'8 aprile 2014, Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238), la Corte ha dichiarato la direttiva 2006/24 invalida.

---

33 V., per analogia, sentenza del 7 settembre 2022, Staatssecretaris van Justitie en Veiligheid (Natura del diritto di soggiorno ai sensi dell'articolo 20 TFUE) (C-624/20, EU:C:2022:639, punti 19 e 20).

---

34 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, punti 99 e 136).

---

35 Inoltre, l'articolo 4, paragrafo 2, TUE stabilisce che la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro. La circostanza che una misura nazionale sia stata adottata a fini di salvaguardia della sicurezza nazionale non comporta l'inapplicabilità del diritto dell'Unione e non dispensa gli Stati membri dal necessario rispetto di

tale diritto. 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, punti 99 e 135).

---

36 Sebbene l'importanza dell'obiettivo di salvaguardia della sicurezza nazionale prevalga su quello della lotta alla criminalità grave, e sia quindi idoneo a giustificare ingerenze più gravi nei diritti fondamentali, detto obiettivo non incide sul diritto degli Stati membri di definire i «reati» o i «reati gravi». 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, punto 136).

---

37 E delle circostanze attenuanti e aggravanti.

---

38 L'avvocato generale Saugmandsgaard Øe ha ritenuto che la legislazione penale e le norme di procedura penale rientrano nella competenza degli Stati membri, sebbene sull'ordinamento giuridico di questi ultimi possano nondimeno incidere le disposizioni del diritto dell'Unione adottate in tale materia, sulla base, segnatamente, dell'articolo 83, paragrafo 2, TFUE. Non sussistono quindi disposizioni di portata generale che forniscano una definizione armonizzata della nozione di «reato grave». Conclusioni nella causa Ministerio Fiscal (C-207/16, EU:C:2018:300, paragrafo 95). L'avvocato generale Pitruzzella ha dichiarato che la definizione di «reato grave» dovrebbe essere lasciata alla valutazione discrezionale degli Stati membri. Infatti, a seconda dei sistemi giuridici nazionali, lo stesso reato può essere sanzionato più o meno severamente. La definizione delle circostanze aggravanti può parimenti variare a seconda degli Stati membri. Conclusioni nella causa Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche) (C-746/18, EU:C:2020:18, paragrafi 91 e 92). Di converso, l'avvocato generale Szpunar ha considerato che «[l]a nozione di "forme gravi di criminalità" deve (...) essere interpretata autonomamente. Essa non può dipendere dalle concezioni di ciascuno Stato membro, salvo permettere un'elusione dei requisiti di cui all'articolo 15, paragrafo 1, della direttiva 2002/58 a seconda che gli Stati membri adottino una concezione estensiva o meno della lotta alle forme gravi di criminalità». Conclusioni nella causa La Quadrature du Net e a (Dati personali e lotta alla contraffazione) (C-470/21, EU:C:2022:838, paragrafo 74).

---

39 Articolo 83, paragrafo 1, primo comma, TFUE.V. anche sentenza del 21 ottobre 2021, Okrazhna prokuratura – Varna (C-845/19 e C-863/19, EU:C:2021:864, punto 32).

---

40 V., per analogia, la sentenza nella causa Prokuratuur, punti 41 e 42. La Corte ha dichiarato che, in assenza di una normativa dell'Unione in materia e in virtù del principio dell'autonomia processuale, «spetta, in linea di principio, al solo diritto nazionale stabilire le regole relative all'ammissibilità e alla valutazione, nell'ambito di un procedimento penale instaurato nei confronti di persone sospettate di atti criminali, di informazioni e di elementi di prova che siano stati ottenuti mediante una conservazione generalizzata e indifferenziata dei dati in questione, contraria al diritto dell'Unione». La base giuridica della direttiva 2002/58 è l'articolo 114 TFUE (ex articolo 95 TCE) e non, ad esempio, l'articolo 83, paragrafo 1, primo comma, TFUE. Di converso, le basi giuridiche della direttiva 2016/681 sono l'articolo 82, paragrafo 1, secondo comma, lettera d), TFUE (cooperazione giudiziaria in materia penale) e l'articolo 87, paragrafo 2, lettera a), TFUE (cooperazione di polizia).

---

41 V. paragrafo 21 delle presenti conclusioni.

---

42 V., per analogia, sentenza del 23 ottobre 2007, Commissione/Consiglio (C-440/05, EU:C:2007:625, punti 66, 70 e 71 nonché giurisprudenza ivi citata). V. anche sentenza del 28 aprile 2011, El Dridi (C-61/11 PPU, EU:C:2011:268, punto 53).

---

43 L'articolo 15, paragrafo 1, della direttiva 2002/58 stabilisce che gli Stati membri «possono adottare» disposizioni legislative che limitano determinati diritti e obblighi previsti da tale direttiva.

---

44 Sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970, punto 89). L'avvocato generale Saugmandsgaard Øe ha dichiarato che, «sebbene ciascuno Stato membro abbia la facoltà di determinare la soglia di pena adeguata per definire grave un reato, esso ha comunque l'obbligo di non fissare tale soglia ad un livello talmente basso, rispetto al quantum abituale delle pene applicabili in tale Stato, che le eccezioni al divieto di

conservare e di utilizzare i dati personali previste da tale articolo 15, paragrafo 1, sarebbero trasformate in principi (...)» conclusioni nella causa Ministerio Fiscal (C-207/16, EU:C:2018:300, paragrafo 114).

45 Nulla indica che la normativa italiana di cui trattasi non rispetti tale principio.

46 Sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a. (C-140/20, EU:C:2022:258, punto 127).

47 V. anche il considerando 11 della direttiva 2002/58.

48 V. anche il considerando 2 della direttiva 2002/58.

49 Sentenze del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970, punto 89) e del 6 ottobre 2020, La Quadrature du Net e a. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punti da 111 a 113). V. anche conclusioni dell'avvocato generale Saugmandsgaard Øe nella causa Ministerio Fiscal (C-207/16, EU:C:2018:300, paragrafi da 116 a 120). Nella sentenza dell'8 marzo 2022, Bezirkshauptmannschaft Hartberg-Fürstenfeld (Effetto diretto) (C-205/20, EU:C:2022:168, punto 31), la Corte ha rammentato che il rispetto del principio di proporzionalità si impone agli Stati membri nell'attuazione del diritto dell'Unione. In siffatto contesto, gli Stati membri sono tenuti ad osservare l'articolo 49, paragrafo 3, della Carta quando adottano sanzioni penali, anche in assenza di una normativa dell'Unione che armonizzi tali sanzioni.

50 Articolo 52, paragrafo 1, della Carta. 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, punto 120).

51 Sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970, punti da 117 a 119). V. anche 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, punti 110 e da 129 a 133).

52 Ad esempio, l'articolo 132, comma 3-bis, del decreto legislativo n. 196/2003 stabilisce norme speciali per l'accesso ai dati in caso di urgenza. Nelle sue conclusioni nella causa La Quadrature du Net e a. (Dati personali e lotta alla contraffazione) (C-470/21, EU:C:2022:838, paragrafi da 99 a 105), l'avvocato generale Szpunar ha ritenuto che un controllo preventivo sia necessario solo in caso di interferenze gravi nella vita privata degli utenti di servizi di comunicazione elettronica. Un controllo preventivo è necessario poiché, nella presente causa, l'ingerenza è grave, a causa della natura dei dati ai quali il pubblico ministero chiede di accedere.

53 È la giurisprudenza della Corte, e non la direttiva 2002/58, ad aver introdotto il requisito del controllo preventivo: sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970, punti 120 e 121 nonché giurisprudenza ivi citata).

54 Sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970, punti 120 e 121).

55 Sentenza Prokuratuur, punto 52.

56 Con riserva di verifica da parte del giudice del rinvio.

57 V. l'analisi contenuta nelle conclusioni dell'avvocato generale Saugmandsgaard Øe nella causa Ministerio Fiscal (C-207/16, EU:C:2018:300, paragrafi da 116 a 120). Si tratta, in ultima analisi, di una questione la cui valutazione spetta al giudice del rinvio.

58 Il fatto che la definizione dei reati e il regime delle sanzioni in uno Stato membro differiscano da quelli adottati in un altro non può, di per sé, ripercuotersi sulla proporzionalità della normativa. V., per analogia, sentenza dell'8 luglio 2010, Sjöberg e Gerdin (C-447/08 e C-448/08, EU:C:2010:415, punto 38).

59 La direttiva 2016/681 riguarda il trasferimento e il trattamento di dati dei passeggeri a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

60 La Corte ha dichiarato che i requisiti derivanti da tale disposizione, che riguardano la natura e la severità della pena applicabile, sono, in linea di principio, idonei a limitare l'applicazione del sistema istituito dalla direttiva 2016/681 a reati che presentino un livello di gravità tale da poter giustificare l'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta. Sentenza del 21 giugno 2022, Ligue des droits humains (C-817/19, EU:C:2022:491, punto 150).

61 La Corte ha quindi statuito che gli Stati membri devono garantire che il sistema istituito dalla direttiva 2016/681 sia limitato alla lotta contro i reati gravi, e non riguardi i reati comuni. Sentenza del 21 giugno 2022, Ligue des droits humains (C-817/19, EU:C:2022:491, punti 151 e 152). L'oggetto e l'ambito di applicazione della direttiva 2016/681, la quale prevede, in particolare, lo scambio di dati PNR fra gli Stati membri, non si sovrappongono a quelli della direttiva 2002/58. Ne consegue che le disposizioni delle suddette direttive devono essere valutate separatamente e in base alle loro caratteristiche intrinseche. A tal riguardo, e a differenza di quanto avviene per l'articolo 15, paragrafo 1, della direttiva 2002/58, la nozione di «reati gravi» di cui alla direttiva 2016/680 è una nozione autonoma del diritto dell'Unione. V. anche, a tal riguardo, considerando 12, articolo 3, punto 9, e allegato II della direttiva 2016/681.

62 V., per analogia, sentenza del 21 giugno 2022, Ligue des droits humains (C-817/19, EU:C:2022:491, punto 151).

63 [Il testo] originale utilizza i termini «i dati sono acquisiti».

64 Fatta salva la verifica da parte del giudice del rinvio, l'utilizzo dell'indicativo all'articolo 132, comma 3, del decreto legislativo n. 196/2003 («i dati sono acquisiti») implica che l'accesso ai dati in parola deve essere concesso dal giudice nazionale, purché siano soddisfatte le condizioni oggettive imposte da tale disposizione.

65 In udienza, le posizioni del pubblico ministero di Bolzano e del governo italiano sul ruolo del giudice nazionale e sulla portata del controllo preventivo ai sensi dell'articolo 132, comma 3, del decreto legislativo n. 196/2003 non coincidevano. Mentre il pubblico ministero ha sostenuto che, prima di concedere l'accesso a siffatti dati, il giudice nazionale è tenuto a effettuare un controllo individuale della proporzionalità della concessione dell'accesso, il governo italiano ha sottolineato che il giudice nazionale è vincolato, conformemente all'articolo 101 della Costituzione della Repubblica Italiana e all'articolo 1 del codice penale, al principio di legalità e, quindi, non può adottare ciò che esso ha descritto come un'interpretazione creativa della legge. Spetta al giudice del rinvio interpretare le disposizioni del diritto nazionale applicabili.

66 Salvo che il diritto nazionale lo consenta e nel rispetto, in particolare, dell'articolo 49 della Carta.

67 Pena della reclusione non inferiore nel massimo a tre anni.

68 L'articolo 52, paragrafo 1, della Carta stabilisce che sia la legge a prevedere eventuali limitazioni all'esercizio di un diritto riconosciuto dalla Carta. Ciò implica che i giudici nazionali sono, in linea di principio, vincolati alla normativa nazionale che prevede siffatte limitazioni.

69 I telefoni cellulari possono contenere fotografie, dati sanitari, estratti bancari, password, ecc. Il furto di un telefono cellulare può quindi pregiudicare l'identità digitale del suo proprietario e i relativi effetti possono essere notevolmente

superiori alla perdita del suo valore monetario. Il giudice del rinvio dovrebbe quindi prendere in considerazione e ponderare anche gli eventuali danni causati ai diritti delle vittime, ai sensi, in particolare, degli articoli 7, 8 e 17 della Carta.

---

70 Come le vittime del reato contestato.

---

71 Con riserva di verifica da parte del giudice del rinvio.

---

72 Numero di registro RGNR 9228/2021.

---

73 Numero di registro RGNR 9794/2021.

---

74 Sebbene i dati possano riguardare comunicazioni effettuate alla vittima dopo la data del furto, essi non riguardano, in realtà, comunicazioni effettuate dalla vittima né dati relativi alla sua ubicazione.

---

75 Secondo il governo italiano, la versione applicabile dell'articolo 269, comma 2, del codice di procedura penale disponeva che «(...) le registrazioni sono conservate fino alla sentenza non più soggetta a impugnazione. Tuttavia gli interessati, a tutela della riservatezza, possono chiedere la distruzione delle registrazioni non acquisite al giudice che ha autorizzato o convalidato l'intercettazione» (perché non rilevanti). Sebbene l'accesso ai dati relativi a terzi innocenti sia illimitato, risulta, salvo verifica da parte del giudice del rinvio, che l'utilizzo di tali dati sia limitato dal diritto nazionale.

---

76 Nella domanda di pronuncia pregiudiziale non si spiega il significato esatto di tale disposizione né la sua applicazione pratica.