



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

CORTE EUROPEA DEI DIRITTI DELL'UOMO

PRIMA SEZIONE

CAUSA ŠKOBERNE c. SLOVENIA

(Ricorso n. 19920/20)

SENTENZA

Art. 6 § 1 (penale) e Art. 6 § 3 lettera d) • Equo processo • Il rigetto del giudice del merito della richiesta del ricorrente di esaminare i due coimputati in qualità di testimoni a seguito della loro ammissione di colpevolezza ha reso iniquo il processo • Richiesta di esame dei coimputati essenzialmente intesa a corroborare la difesa del ricorrente, sufficientemente fondata e pertinente rispetto all'oggetto delle accuse a suo carico • Possibile ritenere la testimonianza dei coimputati in grado di influire sull'esito del processo o di rafforzare la posizione della difesa • Ricorrente privato della possibilità effettiva di addurre e dunque far valere prove testimoniali a sostegno della sua difesa • Insufficiente motivazione da parte dei tribunali interni del rigetto e mancata riparazione dei conseguenti vizi Art. 8 • Vita privata • Corrispondenza • Accesso da parte degli organi di polizia e utilizzo nel procedimento penale a carico del ricorrente dei suoi dati relativi alle telecomunicazioni (dati relativi al traffico e dati relativi all'ubicazione) conservati dai fornitori di telecomunicazioni per un periodo di 14 mesi fissato dalla legge per varie finalità di interesse pubblico • La sorveglianza sistemica comportata dalla conservazione obbligatoria dei dati relativi alle telecomunicazioni rappresentava un impedimento al godimento dei diritti relativi alla vita privata di tutti gli utenti dei servizi di telecomunicazione • La grave natura dell'ingerenza costituita dalla conservazione dei dati impone alla Corte di svolgere un esame più rigoroso per valutare la questione del giusto equilibrio • Assenza di disposizioni o meccanismi mirati a garantire che il provvedimento di conservazione impugnato fosse limitato a quanto "necessario in una società democratica" per conseguire le specifiche finalità elencate dalla pertinente legislazione interna • Dati del ricorrente conservati all'epoca in maniera sistemica, generalizzata e indiscriminata • Regime di conservazione inconciliabile con gli obblighi dello Stato ai sensi dell'art. 8; accesso e utilizzo di tali dati ugualmente non conforme a tale disposizione

Redatta dalla cancelleria. Non vincola la Corte.

STRASBURGO

15 febbraio 2024

DEFINITIVA

15/05/2024

La presente sentenza è divenuta definitiva ai sensi dell'articolo 44 § 2 della Convenzione. Può subire modifiche di forma.

Nella causa Škoberne c. Slovenia,

la Corte europea dei diritti dell'uomo (Prima Sezione), riunita in una Camera composta da:

Alena Poláčková, *Presidente*,
Marko Bošnjak,
Lətif Hüseyinov,
Péter Paczolay,
Ivana Jelić,
Erik Wennerström,
Raffaele Sabato, *giudici*,

e Liv Tigerstedt, *cancelliere aggiunto di Sezione*,

visto il ricorso (n. 19920/20) proposto contro la Repubblica di Slovenia con il quale un cittadino sloveno, il sig. Milko Škoberne ("il ricorrente"), in data 21 aprile 2020, ha adito la Corte ai sensi dell'articolo 34 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali ("la Convenzione");

vista la decisione di comunicare al Governo sloveno ("il Governo") le doglianze concernenti l'articolo 6 (relative all'imparzialità del giudice del merito e al suo rifiuto di consentire l'esame di E.R. e M.S. in qualità di testimoni al processo del ricorrente) e l'articolo 8 della Convenzione e di dichiarare il ricorso irricevibile per il resto;

viste le osservazioni delle parti;

dopo aver deliberato in camera di consiglio in data 23 gennaio 2024,
pronuncia la seguente sentenza, adottata in tale data:

INTRODUZIONE

1. La causa concerne il procedimento penale nei confronti del ricorrente (ex giudice di tribunale distrettuale) nel quale egli era stato condannato per corruzione in atti giudiziari da una giudice che in precedenza aveva accettato l'ammissione di colpevolezza dei suoi due coimputati. Al ricorrente era stata negata la possibilità di esaminare, in qualità di testimoni, tali coimputati a seguito della loro ammissione di colpevolezza. La causa concerne altresì la questione di sapere se sia stato violato l'articolo 8 perché i dati relativi al traffico e all'ubicazione del ricorrente, nel quadro di una misura sistemica, erano stati conservati per un periodo di 14 mesi e utilizzati dalle autorità nel procedimento nei suoi confronti.

IN FATTO

2. Il ricorrente è nato nel 1959 e vive Laško. È stato rappresentato dall'avvocato V. Cugmas, del foro di Slovenske Konjice.

3. Il Governo è stato rappresentato dal suo agente, la sig.ra A. Grum, avvocato dello Stato senior.

4. I fatti della causa si possono riassumere come segue.

I. GLI EVENTI CHE HANNO CONDOTTO AL PROCEDIMENTO PENALE NEI CONFRONTI DEL RICORRENTE

5. Nel 2001 E.Ć. fu condannato dinanzi al Tribunale distrettuale di Celje alla pena di due anni di reclusione per il reato di frode. In seguito egli lasciò il territorio della Slovenia prima che iniziasse l'esecuzione della sua pena detentiva; il 12 dicembre 2007 fu emesso nei suoi confronti un mandato di arresto internazionale ("il mandato di arresto del 2007"). In data 5 novembre 2008 intervenne la prescrizione della pena e in tale data il mandato di arresto del 2007 fu revocato.

6. Contemporaneamente si svolse un altro procedimento penale nei confronti di E.Ć. dinanzi al Tribunale distrettuale di Celje concernente un reato legato alla prostituzione. Il 3 dicembre 2003 fu disposta la sua detenzione. Il 28 maggio 2009 il Tribunale distrettuale di Celje emise un mandato di arresto internazionale nei suoi confronti ("il mandato di arresto del 2009").

7. In data 10 ottobre 2009, E.Ć., mentre cercava di attraversare il confine tra la Croazia e la Bosnia-Erzegovina, fu arrestato sulla base del mandato di arresto del 2009 dalle autorità croate incaricate dell'esecuzione; tuttavia fu rapidamente rilasciato poco dopo. Il ricorrente quel giorno era il giudice istruttore di turno al Tribunale distrettuale di Celje.

8. Ad aprile 2010 E.Ć. presentò al Tribunale distrettuale di Celje una memoria scritta chiedendo che alcune prove fossero espunte dal fascicolo e il procedimento penale nei suoi confronti fosse sospeso.

9. Il 12 novembre 2010, a seguito della richiesta scritta di E.Ć. (che era corroborata da una sua dichiarazione e da alcuni certificati medici relativi alle condizioni di salute della donna che, a suo dire, era la sua compagna) un collegio di tre giudici esterno al tribunale, presieduto dal ricorrente, decise di sospendere la detenzione di E.Ć. e in pari data il ricorrente emise un provvedimento di revoca del mandato di arresto del 2009 a carico di E.Ć.

10. Il 29 novembre 2010, E.Ć. via email sparse una denuncia penale alla polizia nei confronti del ricorrente. Il 14 dicembre 2010 sparse oralmente un'altra denuncia (con ulteriori dettagli) al commissariato di polizia, sostenendo che il ricorrente (con l'aiuto di due intermediari M.S. e E.R.) aveva commesso il reato di corruzione in atti giudiziari e descrivendo l'accaduto come segue. A seguito di accordi presi da E.R. e M.S. egli aveva incontrato il ricorrente, che si era dichiarato potenzialmente disposto ad aiutarlo riguardo al procedimento pendente e ai relativi mandati di arresto (si vedano i paragrafi 5 e 6 *supra*). Dopo il primo incontro (tenutosi in Croazia alla fine del 2008 o all'inizio del 2009 nel quale il ricorrente aveva promesso di occuparsi della faccenda), E.Ć., alla presenza anche di E.R. e M.S., aveva nuovamente incontrato il ricorrente nella primavera del 2009. In

quell'occasione quest'ultimo aveva informato E.Ć. della revoca del mandato di arresto del 2007 (si veda il paragrafo 5 8 *supra*) nonché dell'emissione di un nuovo mandato nei suoi confronti (ovvero del mandato di arresto del 2009, si veda il paragrafo 6 *supra*), e aveva preteso il pagamento dei suoi favori. E.Ć. aveva dato a E.R. 5.000 euro (EUR) (da consegnare al ricorrente). In occasione del terzo incontro, svoltosi nell'estate del 2009 tra le stesse persone del precedente, E.Ć. aveva dato a E.R. EUR 4.000 (da consegnare al ricorrente). Il ricorrente aveva preparato una memoria scritta (che E.Ć. aveva poi presentato al Tribunale distrettuale di Celje, si veda il paragrafo 8 *supra*) e aveva promesso che avrebbe tentato farsi assegnare la causa di E.Ć. A seguito della sospensione della detenzione di E.Ć. e della revoca del mandato di arresto del 2009 (si veda il paragrafo 9 *supra*), il ricorrente aveva preteso altri EUR 50.000 per i suoi favori, minacciando, in caso contrario, l'emissione di un nuovo mandato di arresto nei confronti di E.Ć.

11. Unitamente alla sua denuncia penale, E.Ć. presentò alla polizia diversi elementi di prova e fornì particolari sulle utenze telefoniche utilizzate per le comunicazioni tra i partecipanti durante i summenzionati episodi.

II. LA RACCOLTA DEI DATI, LA SORVEGLIANZA E L'OPERAZIONE SOTTO COPERTURA

12. In data 16 dicembre 2010, il Tribunale distrettuale di Lubiana ordinò ai fornitori di servizi di telecomunicazione interessati di fornire i dati relativi al traffico e all'ubicazione e i collegati dati dell'abbonato (in prosieguo "i dati relativi alle telecomunicazioni") concernenti le utenze telefoniche utilizzate, *inter alia*, da E.Ć. e E.R. relativi al periodo compreso tra il 1° gennaio 2009 e il 16 dicembre 2010. Sulla base dei dati ricevuti dai fornitori di servizi di telecomunicazione (si veda il paragrafo 17 *infra*) la polizia predispose, in data 18 dicembre 2010, un rapporto analitico che stabiliva, *inter alia*, che E.R. nel periodo in questione aveva comunicato con una persona che utilizzava un'utenza telefonica mobile appartenente al Tribunale distrettuale di Celje. In data 20 dicembre 2010, sulla base dello stesso decreto, la polizia predispose un secondo rapporto analitico che riportava i dati relativi alle telecomunicazioni con il dettaglio delle comunicazioni avvenute tra le utenze telefoniche di E.R. e M.S.

13. In data 18 dicembre 2010, il Tribunale distrettuale di Lubiana emise un provvedimento di sorveglianza delle telecomunicazioni (*nadzor telekomunikacij*), ovvero dispose l'intercettazione di diverse utenze telefoniche utilizzate da E.R. e la registrazione delle conversazioni così ottenute.

14. In data 23 dicembre 2010, il Tribunale distrettuale di Lubiana ordinò ai fornitori di servizi di telecomunicazione interessati di fornire i dati relativi alle telecomunicazioni concernenti le utenze telefoniche utilizzate, *inter alia*, da E.R. e M.S. relativamente al periodo compreso tra il 1° gennaio 2009 al 22

dicembre 2010. Sulla base dei dati ricevuti dai fornitori di servizi di telecomunicazione (si veda il paragrafo 17 *infra*) la polizia predispose, in conformità ai decreti del 16 dicembre e del 23 dicembre 2010 del Tribunale distrettuale di Lubiana, un terzo rapporto analitico che riportava i dati relativi alle telecomunicazioni di E.R. e M.S. e a un'utenza telefonica mobile appartenente al Tribunale distrettuale di Celje.

15. In data 27 dicembre 2010, il Tribunale distrettuale di Lubiana emise un provvedimento di sorveglianza delle telecomunicazioni, ovvero dispose l'intercettazione dell'utenza telefonica mobile del Tribunale distrettuale di Celje (che era utilizzata dal ricorrente) e dell'utenza telefonica fissa appartenente e utilizzata dal ricorrente, e la registrazione delle conversazioni così ottenute.

16. In data 12 gennaio 2011, il Tribunale distrettuale di Lubiana ordinò ai fornitori di servizi di telecomunicazione di fornire i dati relativi alle telecomunicazioni concernenti un'utenza telefonica appartenente al Tribunale distrettuale di Celje e utilizzata dal ricorrente. In data 17 gennaio 2011, la polizia predispose un quarto rapporto analitico sulla base dei dati ricevuti dai fornitori di servizi di telecomunicazione (si veda il paragrafo 17 *infra*) in conformità ai decreti del 16 dicembre, 23 dicembre 2010 e 12 gennaio 2011 del Tribunale distrettuale di Lubiana. Tale rapporto, *inter alia*, riportava i dati relativi alle telecomunicazioni concernenti il traffico tra le utenze telefoniche utilizzate dal ricorrente, da E.R. e da M.S.

17. In risposta ai summenzionati decreti del Tribunale distrettuale di Lubiana che disponevano la consegna dei dati relativi alle telecomunicazioni richiesti da parte dei fornitori di servizi di telecomunicazione, questi ultimi spiegarono che essi non potevano fornire le informazioni richieste per tutto il periodo ma soltanto per i quattordici mesi precedenti, il termine minimo di conservazione stabilito dalla pertinente normativa.

18. Durante e successivamente al periodo in cui le summenzionate attività ebbero luogo, fu organizzata un'operazione sotto copertura (con la collaborazione di E.Ć.). Un agente sotto copertura ed E.Ć. sino al 18 febbraio 2011 svolsero operazioni che avevano come obiettivo E.R., M.S. e il ricorrente. E.Ć. partecipò a comunicazioni e a incontri svoltisi in Slovenia con le summenzionate persone. In data 24 gennaio 2011, egli consegnò a E.R. e M.S. una quantità di banconote (i cui numeri di serie erano stati trascritti) pari a una somma di EUR 18.000. Nel corso di successive perquisizioni domiciliari alcune di tali banconote furono rinvenute nelle abitazioni di E.R. e M.S.; il 25 gennaio 2011 il ricorrente versò in banca una somma di denaro liquido (pari a EUR 8.000) che conteneva altre suddette banconote. Nel corso di una perquisizione dell'abitazione del ricorrente furono sequestrati i suoi dispositivi informatici e nel disco rigido del suo computer furono rinvenuti documenti che contenevano la memoria presentata da E.Ć. al Tribunale distrettuale di Celje ad aprile 2010 (si veda il paragrafo 8 *supra*).

19. Il ricorrente E.R. e M.S. furono arrestati il 26 gennaio 2011.

III. L'INDAGINE PENALE CONDOTTA DAL GIUDICE ISTRUTTORE

20. In data 28 gennaio 2011, il ricorrente E.R. e M.S. comparvero dinanzi al giudice istruttore. Il ricorrente si avvalse della facoltà di non rispondere, E.R. scelse di rimanere in silenzio e M.S. rilasciò una dichiarazione in presenza del suo difensore.

21. Nella sua dichiarazione M.S. spiegò che nel 2009 E.R. gli aveva chiesto se conosceva un esperto di diritto in grado di aiutare un suo conoscente (E.Ć.) in relazione a certe questioni legali. M.S. conosceva il ricorrente in quanto erano stati compagni di scuola e così diede a E.R. il suo numero di telefono. E.R. aveva poi contattato il ricorrente direttamente. M.S. riconobbe di aver incontrato E.Ć., E.R. e il ricorrente in Croazia e di aver ricevuto il giorno dell'incidente durante l'attraversamento della frontiera (si veda il paragrafo 7 *supra*) una telefonata da E.Ć. nella quale quest'ultimo gli chiedeva come poter raggiungere il ricorrente menzionando che stava incontrando delle difficoltà per attraversare il confine. Spiegò inoltre che il 24 gennaio 2011 (si veda il paragrafo 18 *supra*) egli, E.R. e E.Ć. si erano incontrati ed egli aveva ricevuto da quest'ultimo una busta contenente la somma di EUR 18.000 in contanti. Aveva poi suddiviso il contante in tre buste (due contenenti EUR 5.000 e una contenente EUR 8.000). Più tardi nella stessa giornata aveva incontrato il ricorrente e gli aveva consegnato la busta contenente EUR 8.000. Insieme al ricorrente aveva poi incontrato E.R. e E.Ć. in un albergo della stessa città. Avevano discusso il rinvio dell'udienza della causa di E.Ć. (si veda il paragrafo 6 *supra*) dovuto all'infermità del giudice o del pubblico ministero. Al momento di lasciare l'albergo, M.S. aveva consegnato una delle buste contenenti EUR 5.000 a E.R.

22. In data 3 febbraio 2011, il giudice istruttore aprì un'indagine nei confronti del ricorrente, di E.R. e di M.S., durante la quale E.Ć. fu interrogato in qualità di persona informata dei fatti.

23. In data 10 gennaio 2012, la Procura depositò un atto di accusa nei confronti del ricorrente, di E.R. e di M.S., imputandoli di aver commesso il reato di corruzione. Furono rigettate le richieste del ricorrente finalizzate all'esclusione di alcune prove, nonché le eccezioni sollevate dal ricorrente, da E.R. e da M.S. contro l'atto di accusa. Nel presentare tali richieste e doglianze il ricorrente non menzionò la conservazione dei dati relativi alle telecomunicazioni da parte dei fornitori di servizi di telecomunicazione in questione né l'utilizzo di tali dati come prove.

IV. IL PROCESSO DINANZI AL TRIBUNALE DISTRETTUALE DI LUBIANA

24. In data 22 novembre e 20 dicembre 2012, il Tribunale distrettuale di Lubiana, in composizione monocratica (giudice V.L.), tenne le udienze

istruttorie nei confronti del ricorrente, di E.R. e di M.S. I loro difensori presentarono richieste finalizzate all'esclusione di alcune prove ma non misero in questione la liceità della conservazione dei dati da parte dei fornitori di servizi di telecomunicazione.

25. In data 14 febbraio 2013, ebbe inizio il processo dinanzi alla giudice V.L. del Tribunale distrettuale di Lubiana. Nella prima udienza il ricorrente dichiarò che avrebbe fornito una dichiarazione difensiva, ma soltanto in una fase successiva del procedimento. Pure M.S. dichiarò che si sarebbe difeso successivamente e anche E.R. si astenne dal difendersi. Il tribunale lesse la dichiarazione resa da M.S. durante l'indagine (si veda il paragrafo 21 *supra*) che fu poi commentata dal ricorrente. Egli sostenne che a M.S. non era stato chiesto se il ricorrente conoscesse le richieste avanzate per suo conto, né perché avesse dato a quest'ultimo EUR 8.000. Il ricorrente affermò inoltre che a M.S. non era stato chiesto se egli e il ricorrente intrattenessero rapporti o affari di altro tipo.

26. Tra il 21 febbraio 2013 e il 5 dicembre 2013, si svolse una serie di ulteriori udienze nel corso delle quali furono acquisite molte prove, *inter alia*, furono ascoltate le registrazioni delle intercettazioni e diversi testimoni che erano stati coinvolti direttamente o indirettamente negli episodi in questione. E.Ć. fu ascoltato anche in qualità di testimone e (diversamente da quanto precedentemente dichiarato durante le indagini e il procedimento seguiti alla denuncia penale) in quell'occasione dichiarò che il denaro che aveva dato a E.R. e che secondo lui quest'ultimo aveva consegnato al ricorrente era destinato a remunerare dei servizi legali e non era un compenso illecito. Disse anche che egli aveva comunicato tale fatto alla polizia quando aveva sporto la sua denuncia penale il 14 dicembre 2010 (si veda il paragrafo 10 *supra*), ma esso non era stato riportato nel verbale. Fornì anche la sua versione dei fatti accaduti al confine croato-bosniaco (si veda il paragrafo 7 *supra*), dichiarando, *inter alia*, che egli aveva mostrato alla polizia di frontiera un documento relativo al mandato di arresto (revocato) del 2007 fornitogli dal ricorrente, senza l'esito sperato, il che aveva spinto la sua compagna a chiamare E.R. Dopo circa trenta o quaranta minuti era stato rilasciato. E.Ć. dichiarò anche che E.R. il giorno dopo l'episodio gli aveva detto che era stato fortunato perché quel giorno era di turno il ricorrente e lo aveva potuto "salvare". Testimoniò inoltre che dopo la revoca del mandato di arresto del 2009 e la sospensione dell'ordinanza di carcerazione, E.R. pretese il versamento di una somma di EUR 50.000, pretesa che ridusse a EUR 40.000 a seguito dei negoziati cui aveva partecipato M.S. Descrisse poi la sua successiva collaborazione con la polizia, che lo aveva incaricato di negoziare il pagamento e lo aveva istruito di consegnare la somma di denaro concordata a condizione che il ricorrente accettasse di incontrarlo di persona. Aveva pagato la somma la sera dello stesso giorno in cui aveva incontrato il ricorrente insieme a M.S. e E.R. (si veda il paragrafo 18 *supra*). Durante il suo esame E.Ć. rispose anche alle domande poste dal ricorrente o dal suo

rappresentante. Disse che il denaro (EUR 9.000) che aveva dato a E.R. e che secondo lui quest'ultimo aveva consegnato al ricorrente, era destinato, nella sua idea, alla remunerazione di servizi legali o di "avvocati". Dichiarò inoltre di essersi rivolto diverse volte al ricorrente, per il tramite di M.S. e E.R., per ricevere consigli relativamente al procedimento pendente nei suoi confronti.

27. Nell'udienza dell'11 dicembre 2013 M.S. e E.R. si dichiararono colpevoli dei reati loro ascritti. La giudice V.L. accettò la loro ammissione di colpevolezza e li dichiarò colpevoli (si veda il paragrafo 35 *infra*). Il ricorrente allora presentò istanza di riconsuazione della giudice V.L. perché sussistevano dubbi in ordine alla sua imparzialità. Il presidente del Tribunale distrettuale di Lubiana rigettò la sua istanza. Osservò che la legge in materia di procedura penale (in prosieguo la "LPP") non prevedeva l'obbligo di astensione del giudice in caso di accettazione dell'ammissione di colpevolezza dei coimputati. La LPP prevedeva invece soltanto (all'articolo 39(2)(3), si veda il paragrafo 56 *infra*) che il giudice o un giurato non potesse pronunciarsi su un atto di accusa, un appello, o un rimedio giudiziario straordinario qualora avesse emesso una decisione di rigetto dell'ammissione di colpevolezza di un imputato o del patteggiamento. Conformemente al principio della presunzione di innocenza, il tribunale in questione doveva determinare separatamente la colpevolezza di ciascun imputato. Spiegò inoltre che per la riconsuazione di un giudice ai sensi dell'articolo 39(1)(6) della LPP (si veda il paragrafo 56 *infra*) occorre la sussistenza di circostanze che suscitassero dubbi in ordine alla sua imparzialità.

28. In data 13 dicembre 2013, il tribunale separò il procedimento nei confronti di E.R. e M.S. da quello nei confronti del ricorrente (si vedano i paragrafi 35-36 *infra*).

29. Nelle udienze del 13 e 19 dicembre 2013 il ricorrente rese dichiarazioni difensive. Spiegò che aveva incontrato E.Ć. per la prima volta in Croazia il 17 novembre 2008 per iniziativa di M.S., che era stato suo compagno di scuola. Confermò che quando si era svolto l'incontro era a conoscenza della pendenza del procedimento penale nei confronti di E.Ć. Secondo il ricorrente, anche E.R. (che egli non conosceva) aveva partecipato all'incontro in quanto amico di vecchia data di E.Ć. Dichiarò anche che aveva spiegato a E.Ć. che egli aveva diritto al gratuito patrocinio ma che qualora non fosse soddisfatto del difensore assegnatogli avrebbe potuto nominarne uno di sua scelta (nel qual caso, però, avrebbe dovuto pagare i suoi servizi). Dichiarò che l'argomento denaro non era stato discusso né allora, né in seguito. In ordine all'ulteriore incontro tra lui E.Ć., M.S. e E.R., il ricorrente dichiarò che era stato M.S. a parlare per la maggior parte del tempo. Affermò che M.S. gli chiese cosa avrebbe fatto se fosse stato lui il giudice della causa di E.Ć. Disse di aver replicato che avrebbe probabilmente sospeso il procedimento, ma che non poteva prendere in carico tale causa perché aveva partecipato a una sua fase precedente e occorreva soddisfare determinate condizioni affinché la causa fosse riassegnata.

30. In ordine all'episodio accaduto il 10 ottobre 2009 alla frontiera tra la Croazia e la Bosnia-Erzegovina (si veda il paragrafo 7 *supra*), il ricorrente dichiarò che M.S. gli aveva detto che E.Ć. era stato "arrestato a un valico di frontiera tra la Bosnia e la Croazia" e che successivamente aveva telefonato di nuovo per comunicargli che E.Ć. era stato rilasciato. Secondo il ricorrente, quando aveva detto a M.S. che egli era di turno il giorno in questione, M.S. aveva replicato "devi averla risolta tu perché [eri] di turno". Il ricorrente dichiarò che tale informazioni era stata evidentemente comunicata a E.Ć.

31. In ordine al denaro, il ricorrente dichiarò che non aveva ricevuto la somma di EUR 9.000 che era stata consegnata a E.Ć. [sic]. Agli incontri non si era parlato di denaro. Quanto alla suddetta somma di EUR 8.000 che aveva ricevuto, il ricorrente dichiarò che gli era stata data come rimborso di un prestito che aveva accordato a M.S. a luglio 2010.

32. All'udienza del 19 dicembre 2013 il difensore del ricorrente chiese di esaminare E.R. e M.S. affermando, *inter alia*, che M.S. poteva fornire informazioni sull'asserito prestito menzionato dal ricorrente nella sua dichiarazione difensiva e che E.R. poteva testimoniare in ordine agli asseriti debiti di E.Ć. verso di lui. Il difensore del ricorrente affermò inoltre che E.R. e M.S. non avevano detto al ricorrente di aver chiesto del denaro a suo nome e che dovevano spiegare le circostanze relative alla questione di tale denaro, ovvero cosa era successo alla somma iniziale di EUR 9.000 e come e perché era stata divisa la somma di EUR 18.000. Il difensore del ricorrente sottolineò anche che E.R. e M.S. non erano più coimputati nello stesso procedimento e potevano quindi essere esaminati in qualità di testimoni nel procedimento nei confronti del ricorrente. Secondo il difensore del ricorrente E.R. e M.S., a seguito delle loro ammissioni di colpevolezza e della loro condanna, erano divenuti testimoni incriminanti (ovvero testimoni a carico dell'imputato); il ricorrente non poté porre domande a M.S. (che aveva reso una testimonianza che lo incriminava e aveva successivamente rinunciato a difendersi) o esaminare E.R. (che era assente).

33. All'udienza del 19 dicembre 2013 la giudice V.L. rigettò la richiesta presentata dal difensore del ricorrente affinché consentisse l'esame di E.R. e M.S. La giudice argomentò che entrambe tali persone avevano ancora la qualità di imputato perché la sentenza nei loro confronti non era ancora divenuta definitiva. Dichiarò che erano state presentate prove sufficienti a consentire una decisione in ordine alle accuse a carico del ricorrente. Aggiunse che non era possibile chiarire con E.R. e M.S. le ragioni o i motivi delle loro rispettive ammissioni di colpevolezza perché ciò avrebbe violato i loro diritti legali.

34. Successivamente il ricorrente reiterò la sua richiesta di esame di E.R. e M.S., sostenendo che l'udienza avrebbe dovuto essere rinviata sino a quando la sentenza nei confronti di E.R. e M.S. fosse passata in giudicato e affermando che tale esame avrebbe fornito prove importantissime per la sua difesa. La giudice V.L. rigettò nuovamente la richiesta. Nella sentenza nei

confronti del ricorrente (si veda il paragrafo 37 *infra*) addusse due motivi. In primo luogo, ritenne che al momento del vaglio della richiesta di esame di E.R. e M.S. la sentenza nei loro confronti non fosse ancora definitiva, né era certo che lo sarebbe divenuta dopo la scadenza del termine per dichiarare l'intenzione di impugnarla. Secondo la pertinente giurisprudenza interna, i coimputati, anche quando erano giudicati in un procedimento separato, non potevano essere esaminati in qualità di testimoni in un procedimento nei confronti di altri coimputati a meno che la sentenza nei loro confronti non fosse divenuta definitiva. In secondo luogo, la giudice ritenne che l'esame dei coimputati non potesse avere un effetto determinante sulla sua valutazione delle prove già esaminate. Osservò che il tribunale non aveva fondato la propria valutazione delle prove ad esso sottoposte sulle ammissioni di colpevolezza di E.R. e M.S. o sulla dichiarazione resa da M.S. (che era stata letta al processo). Osservò ancora che anche se M.S. non si fosse difeso dinanzi al giudice istruttore e non fossero state accettate le ammissioni di colpevolezza di E.R. e M.S., ella avrebbe condannato il ricorrente sulla base delle numerose prove raccolte a prescindere da tali ammissioni. La giudice osservò inoltre che il ricorrente aveva potuto presentare commenti relativamente alla dichiarazione (contenente alcune affermazioni incriminanti) resa da M.S. durante le indagini e non ritenne convincente la sua difesa tardiva: egli avrebbe potuto presentare le prove pertinenti in una fase precedente del procedimento.

V. LA SENTENZA NEI CONFRONTI DI E.R. E M.S.

35. In data 16 dicembre 2013 la giudice V.L. condannò E.R. e M.S. sulla base delle loro rispettive ammissioni di colpevolezza infliggendo loro una pena detentiva sospesa e una multa pari a circa EUR 3.000 ciascuno. Furono ritenuti colpevoli del reato continuato di accettazione di un compenso illecito allo scopo di "favorire la corruzione di un pubblico ufficiale che chiedeva e accettava compensi per abusare del suo ufficio". Nella sentenza si dichiarava che E.R. e M.S. avevano ciascuno favorito "la corruzione di un pubblico ufficiale, il giudice Milka Škoberneta", e si indicavano i seguenti atti mediante i quali detto reato era stato commesso:

- E.R. e M.S. avevano organizzato tre incontri con E.Ć. e il ricorrente nel 2009.
- E.R. aveva chiesto e ottenuto a nome del ricorrente EUR 9.000 da E.Ć.
- E.R. e M.S. avevano informato il ricorrente della situazione in cui si era trovato E.Ć. al valico di frontiera (si veda il paragrafo 7 *supra*), dopo di che il ricorrente, in qualità di giudice istruttore del Tribunale distrettuale di Celje di turno quel giorno, era intervenuto inviando il provvedimento di revoca del mandato di arresto del 2007 (che in realtà era irrilevante per la situazione in questione) assicurando in tal modo il rilascio di E.Ć.

- E.R. era intervenuto in modo tale (*posreduje pri*) che il ricorrente aveva preparato una memoria scritta affinché E.Ć. la presentasse al Tribunale distrettuale di Celje, la quale grazie alla sua assistenza era stata inserita nel fascicolo (si veda il paragrafo 8 *supra*); inoltre E.R. aveva trasmesso a E.Ć. alcune memorie preparate dal ricorrente destinate ad agevolare la decisione di sospendere la sua detenzione e la revoca del mandato di arresto del 2009 (si veda il paragrafo 9 *supra*); E.R. era anche intervenuto per assicurarsi che E.Ć. firmasse la memoria e si era procurato le prove (di cui conosceva la natura fuorviante) richieste dal ricorrente.

- E.R. e M.S. avevano preteso prima EUR 50.000, e poi EUR 40.000 da E.Ć. allo scopo di ottenere un compenso per il ricorrente e per la loro assistenza, e di ciò avevano discusso per telefono e negli incontri con E.Ć. (informandone il ricorrente).

- E.R. e M.S. avevano ricevuto da E.Ć. per sé stessi e per il ricorrente un compenso illecito pari a EUR 18.000.

36. La sentenza nei confronti di M.S. e E.R. divenne definitiva il 25 dicembre 2013 allo scadere del termine di otto giorni entro il quale E.R. e M.S. avrebbero potuto dichiarare (ma non lo avevano fatto) la loro intenzione di impugnarla.

VI. SENTENZE NEI CONFRONTI DEL RICORRENTE

A. La sentenza del Tribunale distrettuale di Lubiana

37. In data 23 dicembre 2013 la giudice V.L. del Tribunale distrettuale di Lubiana dichiarò il ricorrente colpevole del reato continuato di corruzione in atti giudiziari (la giudice V.L. ritenne che il ricorrente, in qualità di giudice distrettuale del Tribunale distrettuale di Celje e quindi di pubblico ufficiale, aveva chiesto e accettato un compenso per abusare del suo ufficio nell'esercizio dei suoi poteri ufficiali).

38. La giudice V.L. stabilì, *inter alia*, che: il ricorrente aveva promesso a E.Ć. che avrebbe tentato di prendere in carico l'esame della sua causa (si veda il paragrafo 10 *supra*) e di porre fine al procedimento nei suoi confronti; gli aveva promesso che avrebbe tentato di ottenere la revoca del mandato di arresto del 2009 (si veda il paragrafo 6 *supra*); aveva preparato per E.Ć. la memoria scritta depositata ad aprile 2010 (si veda il paragrafo 8 *supra*); era intervenuto (nel suo ruolo di giudice istruttore di turno) per ottenere il rilascio di E.Ć. al valico di frontiera tra la Croazia e la Bosnia (si veda il paragrafo 7 *supra*) inviando un provvedimento che egli sapeva non riguardare il mandato di arresto servito da fondamento della sua detenzione (il mandato di arresto del 2009) bensì invece il mandato di arresto del 2007 (revocato) e aveva presieduto il collegio esterno al tribunale che aveva sospeso la detenzione di E.Ć. e aveva poi revocato il mandato d'arresto sulla base di una richiesta scritta e di altri documenti che erano stati predisposti per conto di E.Ć. o erano

stati sollecitati dal ricorrente (che sapeva che le informazioni ivi contenute erano inesatte, si veda il paragrafo 9 *supra*). La giudice V.L. stabilì che, quale compenso per i suddetti atti, il ricorrente, con l'assistenza di E.R. e M.S. e in concorso con loro, aveva preteso e ricevuto da E.Ć., in data compresa tra novembre 2008 e giugno 2009, la somma di EUR 9.000. Ritenne inoltre che il ricorrente, in concorso con E.R. e M.S., avesse successivamente preteso, in data compresa tra il 14 novembre 2010 e il 24 gennaio 2011, la somma di EUR 50.000 o EUR 40.000, ricevendone, in concorso con E.R. e M.S., EUR 18.000 in data 24 gennaio 2011.

39. Per pervenire a tali conclusioni il tribunale fece riferimento alle dichiarazioni di E.Ć. alla polizia nelle quali egli aveva descritto gli incontri avvenuti in Croazia e le ritenne corroborate dalla dichiarazione resa da M.S. durante le indagini (si vedano i paragrafi 10 e 21 *supra*). Fece altresì riferimento ai dati relativi alle telecomunicazioni che erano stati procurati dai fornitori di servizi di telecomunicazione coinvolti ed erano stati analizzati dalla polizia (si vedano i paragrafi 12, 14 e 16 *supra*), che, secondo il tribunale, corroboravano gli elementi di prova inizialmente forniti da E.Ć. In particolare, il tribunale fece riferimento all'analisi che mostrava che avevano avuto luogo comunicazioni tra E.R., M.S., E.Ć. e il ricorrente il giorno del summenzionato episodio al valico di frontiera (si veda il paragrafo 7 *supra*) e alla decisione del collegio esterno al tribunale in merito alla detenzione di E.Ć. (si veda il paragrafo 9 *supra*). In ordine alla conclusione secondo la quale il ricorrente aveva promesso di intervenire nella procedura legale riguardante E.Ć. (prevedendo di ricevere del denaro quale compenso) il tribunale fece riferimento anche alle comunicazioni registrate grazie alle intercettazioni e ai risultati dell'operazione sotto copertura. Per esempio, in una delle conversazioni registrate M.S. diceva che E.Ć. aveva consegnato EUR 9.000, pensando che la questione fosse risolta. Durante l'incontro del 24 gennaio 2011 era stato registrato il ricorrente mentre spiegava che era di turno il giorno dell'incidente al valico di frontiera (si veda il paragrafo 7 *supra*) e che egli aveva inviato il mandato di arresto del 2007 revocato. In ordine a tale episodio il Tribunale citò anche la dichiarazione di M.S. (si veda il paragrafo 21 *supra*) nella quale egli aveva affermato che E.R. quel giorno lo aveva chiamato chiedendogli come avrebbe potuto raggiungere il ricorrente.

40. In ordine ai fatti seguiti alla sospensione della detenzione di E.Ć. e alla revoca del mandato d'arresto del 2009 (si veda il paragrafo 9 *supra*), il tribunale fece riferimento, *inter alia*, alle seguenti prove. In diverse occasioni erano state registrate conversazioni in cui M.S. e E.R. discutevano gli sviluppi del procedimento penale nei confronti di E.Ć. (si veda il paragrafo 6 *supra*) ed esprimevano la loro frustrazione per il mancato pagamento da parte dello stesso delle somme richieste. Menzionavano spesso il ricorrente come qualcuno che era stato consultato o coinvolto nella discussione della causa penale di E.Ć. Le registrazioni delle conversazioni tra E.R. e il ricorrente mostravano che E.R. (durante un incontro con E.Ć. tenutosi il 31 dicembre

2010) aveva telefonato al ricorrente informandolo che “le cose [si stavano] muovendo in una direzione leggermente migliore”. Il tribunale citò anche una serie di conversazioni registrate tra E.R. e E.Ć. in cui il primo chiedeva al secondo di pagare, al che quest’ultimo (che stava agendo nel quadro dell’operazione sotto copertura) aveva insistito per incontrare il ricorrente. La registrazione di una successiva conversazione svoltasi tra M.S. e il ricorrente il 7 gennaio 2011 dimostrava che il primo aveva informato il secondo che “lui” voleva incontrarlo, e il ricorrente aveva acconsentito. Durante l’incontro dell’8 gennaio 2011 tra E.R., E.Ć. e M.S., quest’ultimo aveva detto che il ricorrente non poteva incontrare in pubblico gli imputati e che con questo non si poteva “scherzare”. Il tribunale citò anche le successive conversazioni tra il ricorrente e M.S. nelle quali quest’ultimo era stato registrato mentre diceva che “lui” stava ancora contrattando e voleva incontrare il ricorrente e che “lui” si stava ammorbidente. Durante una di tali conversazioni era stati anche menzionati eventi accaduti durante il procedimento penale che apparentemente erano riferiti a E.Ć. Durante il summenzionato incontro del 24 gennaio 2011 (si veda il paragrafo 18 *supra*) il ricorrente era stato registrato mentre replicava a E.Ć. (che spiegava le difficoltà incontrate per raccogliere il denaro) che tali difficoltà non erano un problema. Quanto alla suddivisione del denaro consegnato il 24 gennaio 2011, il tribunale citò la dichiarazione di M.S. (si veda il paragrafo 21 *supra*) e la registrazione di una conversazione tra costui e E.R. in cui M.S. aveva proposto di suddividere il denaro in un rapporto “5 e 5 a 8”.

41. Secondo il tribunale le conversazioni registrate indicavano che il ricorrente era al corrente del pagamento richiesto e del suo scopo. Il tribunale concluse pertanto che la dichiarazione del ricorrente secondo la quale il denaro ricevuto da M.S. costituiva il rimborso di un prestito (si veda il paragrafo 31 *supra*) era “soltanto un mezzo di difesa”. A tale proposito il tribunale osservò anche che il ricorrente non aveva dimostrato in maniera convincente in che modo avesse ottenuto il denaro all’epoca in cui asseritamente lo aveva prestato a M.S. In ordine alla modifica della deposizione di E.Ć. il tribunale osservò che le sue dichiarazioni al processo (si veda il paragrafo 26 *supra*) non erano credibili e che era anche possibile che egli fosse stato influenzato dalle minacce che aveva ricevuto durante il procedimento.

42. Il ricorrente fu condannato a cinque anni e sei mesi di reclusione e a una multa di quasi EUR 20.000; fu altresì condannato al pagamento di EUR 12.000, somma corrispondente al vantaggio economico ottenuto dal reato commesso.

B. La sentenza del Tribunale superiore di Lubiana

43. Il ricorrente impugnò la sentenza del tribunale di primo grado in ragione del fatto che E.R. e M.S. non erano stati esaminati e la giudice V.L.,

pur avendo accettato le loro ammissioni di colpevolezza, non si era astenuta. Il ricorrente affermò di non aver mai preteso o ricevuto denaro da E.Ć., e che con la consegna di EUR 8.000 M.S. aveva semplicemente rimborsato un prestito. Dedusse inoltre che il tribunale di primo grado nel condannarlo e nel motivare i decreti finalizzati all'acquisizione di altre prove si era basato sui dati relativi alle telecomunicazioni che erano stati conservati in conformità a un regime giuridico che era stato dichiarato invalido e che era contrario, *inter alia*, all'articolo 8 della Convenzione. A tale proposito invocò la sentenza del 3 luglio 2014 della Corte costituzionale e la sentenza pronunciata dalla Corte di giustizia dell'Unione europea (CGUE) nella causa *Digital Rights Ireland e altri* (si vedano i paragrafi 66-68 e 74-76 *infra*) e sottolineò il carattere indiscriminato e generalizzato del regime di conservazione dei dati in questione.

44. Con sentenza del 22 settembre 2014, il Tribunale superiore di Lubiana rigettò l'appello del ricorrente confermando le conclusioni del Tribunale distrettuale di Lubiana. In ordine al rigetto della richiesta di esame di E.R. e M.S. il Tribunale superiore di Lubiana ritenne che fosse incontestabile che E.R. e M.S. non potessero essere esaminati in qualità di testimoni sino a quando la sentenza nei loro confronti non fosse divenuta definitiva. La sentenza nei confronti del ricorrente era stata pronunciata prima di tale accadimento. Suddetto tribunale ritenne inoltre che il ricorrente non avesse dimostrato con un grado di probabilità sufficiente che le testimonianze eventualmente rese da E.R. e M.S. avrebbero potuto scardinare le conclusioni del tribunale. Quanto alla mancata ricusazione della giudice V.L., il Tribunale superiore di Lubiana ritenne che la LPP in tale situazione procedurale (niente affatto infrequente) non prevedesse l'obbligo di ricusazione del giudice. Osservò che prima di accettare le ammissioni di colpevolezza il tribunale aveva dovuto valutare se esse fossero inequivoche e corroborate dalle prove presenti nel fascicolo (si veda il paragrafo 58 *infra*).

45. In ordine alla raccolta dei dati, il Tribunale superiore di Lubiana osservò che la decisione della Corte costituzionale non era intervenuta sull'articolo 149.b della LPP (si veda il paragrafo 57 *infra*) e non aveva indicato che i dati in possesso delle autorità prima della pronuncia dovessero essere distrutti. Rinviano alla decisione della Corte costituzionale (si vedano i paragrafi 66-68 *infra*) e a quella della CGUE (si vedano i paragrafi 74-76 *infra*), il Tribunale superiore di Lubiana constatò che nel caso di specie era stato accertato un sospetto di grado sufficiente (come previsto dall'articolo 149.b della LPP (si veda il paragrafo 57 *infra*)) a far ritenere il ricorrente coinvolto in un reato prima dell'acquisizione dei dati relativi alle telecomunicazioni e che successivamente tale sospetto non aveva fatto che crescere. I decreti che autorizzavano l'accesso avevano riguardato persone specifiche e specifiche utenze telefoniche mobili. Soltanto uno dei quattro rapporti analitici prodotti dalla polizia sulla base dei dati relativi alle telecomunicazioni raccolti (ovvero quello del 17 gennaio 2011) riguardava il

ricorrente. Il numero in questione apparteneva a un'utenza telefonica del Tribunale distrettuale di Celje (ovvero, di un'istituzione dello Stato), il che diminuiva la gravità dell'asserita intrusione nella vita privata del ricorrente. Il Tribunale superiore di Lubiana esaminò poi la proporzionalità dell'ingerenza tenendo conto della natura e della gravità dei reati di corruzione e concluse che le misure in questione erano state necessarie.

C. La sentenza della Corte suprema

46. Il ricorrente propose ricorso per la tutela della legalità, lamentando, *inter alia*, che il rifiuto del tribunale di primo grado di consentire l'esame di E.R. e M.S. aveva violato i suoi diritti ai sensi dell'articolo 6, compreso il suo diritto (ai sensi dell'articolo 6 § 3 lettera d)) di esaminare i testimoni a suo carico. Il tribunale avrebbe potuto rinviare l'udienza fino a quando la sentenza nei confronti di E.R. e M.S. non fosse passata in giudicato. L'articolo 6 era stato violato anche perché la giudice V.L. non si era astenuta dal presiedere il procedimento dinanzi al tribunale di primo grado. La LPP, che non prevedeva l'obbligo di astensione del giudice in caso di insorgenza di tale situazione procedurale, era contraria alla Costituzione. Inoltre, invocando (i) la decisione della Corte costituzionale del 3 luglio 2014 che concerneva disposizioni identiche a quelle su cui si basava la conservazione dei dati relativi alle telecomunicazioni nel suo caso e (ii) la sentenza della CGUE nella causa *Digital Rights Ireland e altri* (si vedano i paragrafi 66-68 e 74-76 *infra*), il ricorrente sostenne che la conservazione e il successivo utilizzo dei dati relativi alle telecomunicazioni avevano violato la Convenzione, la Costituzione e il pertinente diritto dell'Unione europea, e che per giunta erano sproporzionati. Affermò che, nel valutare la liceità della conservazione e dell'accesso ai dati in questione da parte delle autorità, la sentenza del Tribunale superiore di Lubiana aveva contraddetto le conclusioni delle summenzionate corti. Il ricorrente lamentò di essere stato condannato sulla base di dati relativi alle telecomunicazioni che erano stati ottenuti violando i suoi diritti relativi alla vita privata e di prove che erano state ricavate da tali dati.

47. Il ricorrente sottolineò anche che la Corte suprema nel procedimento disciplinare nei suoi confronti, con decisione del 17 ottobre 2014, aveva concluso che il regime di conservazione previsto dalla legge del 2004 come modificata (si veda il paragrafo 64 *infra*), che era identico a quello previsto dalla legge del 2012 (si veda il paragrafo 65 *infra*), era incostituzionale. Citò inoltre il fatto che la Corte suprema in quel procedimento aveva escluso dal fascicolo i rapporti analitici predisposti sulla base dei dati relativi alle telecomunicazioni conservati e aveva ordinato al tribunale di grado inferiore di stabilire l'incidenza di tali rapporti sull'ammissibilità delle relative prove.

48. In data 9 giugno 2015 la Corte suprema rigettò il ricorso per la tutela della legalità del ricorrente. In ordine al rigetto della sua richiesta di esame di

E.R. e M.S. la Corte suprema seguì il ragionamento dei tribunali inferiori. Osservò che al momento della presentazione della richiesta era impossibile prevedere che le condanne di E.R. e M.S. non sarebbero state impugnate. Osservò inoltre che il ricorrente aveva presentato la sua difesa (quando aveva sollevato nuove questioni fattuali) soltanto più avanti nel procedimento.

49. La Corte suprema sottolineò anche che durante il procedimento E.R. non aveva voluto difendersi e aveva invocato il suo diritto al silenzio. Quanto a M.S., la difesa era stata informata della sua dichiarazione non più tardi del 3 febbraio 2011, data di inizio delle indagini (si veda il paragrafo 22 *supra*) ma ciononostante non aveva chiesto il suo esame durante il processo. A prescindere da ciò, il tribunale di primo grado non aveva potuto fondare la propria sentenza esclusivamente o in misura determinante sulla testimonianza di M.S.

50. In ordine alla mancata ricusazione della giudice V.L., la Corte suprema ritenne che quando i coimputati avevano ammesso la propria colpevolezza appena prima che terminasse l'assunzione delle prove, ciò di per sé non giustificasse la ricusazione del giudice ai sensi dell'articolo 39(1)(6) della LPP (si veda il paragrafo 56 *infra*). Concordò con il Tribunale superiore di Lubiana sul fatto che il legislatore evidentemente non aveva considerato la situazione in cui il giudice poteva respingere un'ammissione di colpevolezza o un patteggiamento paragonabile alla situazione in cui l'accettava. Sottolineò inoltre che il giudice doveva decidere in base alle prove sulla colpevolezza e sulle pene in relazione a ciascun imputato separatamente, e nel farlo doveva considerare anche le (eventuali) ammissioni di colpevolezza alla luce delle altre prove assunte. La Corte suprema osservò anche che il ricorrente non aveva proposto all'esame nessun'altra circostanza in grado di sollevare dubbi sull'imparzialità della giudice V.L.

51. In ordine alla conservazione e all'utilizzo dei dati relativi alle telecomunicazioni, la Corte suprema osservò che i dati in questione erano stati acquisiti in virtù di un decreto del tribunale emesso in conformità all'articolo 149.b della LPP (si veda il paragrafo 57 *infra*), che non era stato dichiarato invalido dalla Corte costituzionale. Secondo la Corte suprema la decisione della Corte costituzionale in questione (si vedano i paragrafi 66-68 *infra*) non aveva avuto effetto sui dati raccolti e acquisiti prima di tale pronuncia. La Corte suprema osservò inoltre che la Corte costituzionale non aveva annullato la disposizione ai sensi della quale il tribunale doveva conservare i dati acquisiti per tutto il tempo di conservazione del fascicolo penale. I dati in questione erano stati acquisiti e conservati oltre tre anni prima della pronuncia della summenzionata sentenza della CGUE e della decisione della Corte costituzionale (si vedano i paragrafi 66-68 e 74-76 *infra*). La Corte suprema ritenne poi che la consultazione e il trattamento dei dati da parte delle autorità non avesse costituito una misura indiscriminata e preventiva. Il decreto che disponeva l'acquisizione dei dati relativi alle telecomunicazioni

era limitato al periodo in esame ed era basato sulla sussistenza di motivi per sospettare che il ricorrente avesse commesso il reato dedotto e sui fatti e le informazioni incriminanti già precedentemente in possesso delle autorità. Osservò inoltre che nei confronti del ricorrente erano state disposte misure di sorveglianza segreta come per esempio le intercettazioni (che dovevano essere fondate su un ragionevole sospetto, un criterio di prova più rigoroso dei motivi di sospetto richiesti per concedere l'accesso ai dati relativi alle comunicazioni) e che il successivo decreto di acquisizione dei dati relativi alle telecomunicazioni aveva costituito un'ingerenza di minore portata nel suo diritto alla riservatezza delle comunicazioni. Concluse che le misure adottate nei confronti del ricorrente non avevano costituito un'ingerenza sproporzionata nel suo diritto alla riservatezza delle comunicazioni e alla protezione dei dati personali (garantiti dalla Costituzione) e che non vi erano pertanto motivi per ritenere che il procedimento penale impugnato si fosse svolto in maniera contraria alle norme procedurali fondamentali.

D. La decisione della Corte costituzionale

52. Il ricorrente propose due doglianze costituzionali. Lamentò, *inter alia*, il rifiuto di consentire l'esame di E.R. e M.S., che aveva asseritamente violato i suoi diritti di difesa, e la mancata ricusazione della giudice V.L. Lamentò inoltre che non sussisteva alcun fondamento costituzionalmente ammissibile per la conservazione non selettiva dei dati relativi alle telecomunicazioni da parte dei fornitori di servizi di telecomunicazione in questione. Il ricorrente reiterò e approfondì ulteriormente i rilievi proposti nei precedenti ricorsi. Sottolineò l'asserita discrepanza tra le posizioni assunte dalla Corte suprema nel procedimento penale e in quello disciplinare (si veda il paragrafo 47 *supra*) e sostenne che la conservazione e il trattamento dei suoi dati relativi alle telecomunicazioni non avrebbero dovuto essere esaminati attraverso la lente dell'articolo 149.b della LPP perché tali dati erano stati conservati illegalmente in virtù di un regime che era stato dichiarato invalido a causa del suo carattere sproporzionato. L'accesso a tali dati e la loro conservazione nel fascicolo non potevano trasformare dati conservati illegalmente in dati conformi al dettato costituzionale. Citò l'articolo 18 della LPP che stabiliva che nessuna decisione giudiziaria poteva essere fondata su prove ottenute violando i diritti umani garantiti dalla Costituzione.

53. In data 24 settembre 2018 la Corte costituzionale accettò di esaminare le doglianze costituzionali del ricorrente e in data 9 ottobre 2019 le rigettò nel merito. In ordine al rigetto della richiesta di esame di E.R. e M.S., ritenne convincenti le decisioni dei tribunali inferiori. Secondo tale corte era fondamentale osservare che E.R. aveva optato per il silenzio e che la condanna del ricorrente non era fondata esclusivamente o in misura determinante sulla dichiarazione di M.S.

54. In ordine alla mancata ricusazione della giudice V.L., la Corte costituzionale ritenne che gli atti dei coimputati del ricorrente (che avevano funto da intermediari della corruzione) e del ricorrente (la persona che aveva sollecitato il compenso illecito) traessero origine dallo stesso evento passato; infatti, tali atti comportavano forme diverse di concorso nel medesimo reato. La Corte costituzionale ritenne evidente che gli atti degli intermediari fossero collegati a quelli del pubblico ufficiale (ovvero il ricorrente) che aveva sollecitato o accettato il compenso illecito e che l'atto di quest'ultimo avesse costituito il prerequisite per l'accertamento della responsabilità penale degli intermediari e della sussistenza della corruzione. Ad ogni modo, la sentenza basata sull'ammissione di colpevolezza di E.R. e M.S. aveva riguardato soltanto i coimputati del ricorrente (che avevano ammesso la loro colpevolezza). La Corte costituzionale osservò inoltre che il valore epistemico di un'ammissione di colpevolezza (ovvero la sua incidenza sulla valutazione della causa) dipendeva dalla fase del procedimento in questione in cui essa era effettuata; tanto più tardi essa interveniva nel corso della raccolta delle prove tanto minore era il peso che aveva sul processo cognitivo del giudice. I coimputati effettuarono la loro ammissione di colpevolezza soltanto nel corso della diciannovesima udienza del processo, quando l'assunzione delle prove era entrata nella fase finale ed era stata quasi completata. Secondo la Corte costituzionale non si poteva pertanto ritenere che la giudice V.L. si fosse formata un'opinione preconcepita della colpevolezza del ricorrente a causa delle ammissioni dei suoi coimputati. Sebbene la sentenza, che era basata sulle ammissioni di colpevolezza di E.R. e M.S., implicasse che la giudice V.L. fosse convinta della loro colpevolezza e avesse menzionato il ruolo del ricorrente, essa non aveva citato alcuna opinione del tribunale riguardo alla colpevolezza del ricorrente, né il tribunale nella sentenza nei confronti del ricorrente aveva citato le ammissioni di colpevolezza dei coimputati. Conseguentemente la Corte costituzionale concluse che il diritto del ricorrente a che la sua causa fosse esaminata da un giudice imparziale non era stato violato.

55. In ordine alla conservazione e all'utilizzo dei dati relativi alle telecomunicazioni, la Corte costituzionale osservò che i dati acquisiti nella causa del ricorrente avevano consentito di formulare conclusioni sul luogo, l'ora, la durata e il tipo di comunicazioni, e di sapere "chi aveva chiamato chi". I dati acquisiti avevano consentito di pervenire a conclusioni dettagliate sulla vita privata del ricorrente, dei coimputati e della parte lesa. La Corte costituzionale sottolineò che sia la sua precedente decisione che la sentenza della CGUE nella causa *Digital Rights Ireland e altri* (si vedano i paragrafi 66-68 e 74-76 *infra*) avevano riguardato la conservazione e non l'accesso ai dati. L'accesso ai dati, pertanto, non poteva essere valutato con i criteri stabiliti da tali due decisioni. La Corte costituzionale esaminò poi la proporzionalità dell'ingerenza nella riservatezza delle comunicazioni del ricorrente prodotta dall'accesso ai suoi dati da parte delle autorità. Concluse

che nei decreti che autorizzavano l'accesso il tribunale di primo grado aveva stabilito (come richiesto dalla legge) la sussistenza di motivi per sospettare che era stato commesso un reato e la necessità di accedere ai dati relativi alle telecomunicazioni ai fini delle indagini su tale reato. Osservò inoltre che il ricorrente non aveva dedotto l'inosservanza delle condizioni previste dall'articolo 149.b della LPP per ottenere l'accesso. La Corte costituzionale osservò poi che il reato in questione era un reato di corruzione di grave natura. In ordine alla questione della durata della misura la Corte costituzionale prese in considerazione il periodo di tempo in cui le autorità avevano avuto accesso ai dati. Fece riferimento ai periodi stabiliti dall'articolo 107.a della legge del 2004, come modificata, osservando che tale disposizione era sostanzialmente la stessa disposizione contenuta nella legge del 2012 (si veda il paragrafo 65 *infra*) che era stata dichiarata invalida con decisione del 3 luglio 2014. Osservò inoltre che i dati potevano essere conservati per un certo periodo anche in "strutture commerciali" ai sensi dell'articolo 104 della legge del 2004, come modificata (si veda il paragrafo 64 *infra*). Osservò poi che i dati in questione erano stati acquisiti diversi anni prima della pubblicazione della propria decisione del 3 luglio 2014 (si vedano i paragrafi 66-68 *infra*). Inoltre, anche se i dati acquisiti nel procedimento penale nei confronti del ricorrente erano relativi al suindicato periodo di quattordici mesi e i quattro rapporti analitici avevano almeno indirettamente incriminato il ricorrente, il Tribunale distrettuale di Lubiana aveva fatto riferimento a un ventaglio ristretto di dati acquisiti per corroborare la testimonianza di E.Ć. e negare la credibilità della difesa del ricorrente. Tali dati riguardavano specifiche comunicazioni telefoniche che avevano avuto luogo soltanto un mese e quattro giorni prima dell'emissione del primo decreto che autorizzava l'accesso e due mesi prima dell'emissione dell'ultimo decreto di tale tipo. La Corte costituzionale ritenne pertanto probabile che i dati relativi alle telecomunicazioni direttamente citati nella sentenza del tribunale di primo grado fossero stati conservati per il periodo concesso alle "strutture commerciali". Secondo la Corte costituzionale, tale fatto era rilevante anche per la valutazione della proporzionalità della misura, in quanto riduceva l'importanza dell'intrusione nei diritti del ricorrente. La Corte costituzionale concluse che gli altri tribunali avevano correttamente giustificato l'ingerenza nel diritto del ricorrente alla riservatezza delle comunicazioni e non potevano essere accusati di non aver conseguito un ragionevole equilibrio tra tale diritto e gli interessi del procedimento penale.

IL QUADRO GIURIDICO E LA PRASSI PERTINENTI

I. IL DIRITTO E LA PRASSI INTERNI PERTINENTI

A. La legge in materia di proceduta penale

56. La legge in materia di proceduta penale, entrata in vigore il 1° gennaio 1995, con le relative modifiche, all'articolo 39 (intitolato "esclusione") stabilisce quanto segue:

“(1) Un giudice o un giudice popolare non può svolgere la funzione giudiziaria

(...)

4) qualora in relazione alla stessa questione abbia [già] agito in qualità di pubblico ministero, difensore (...) [o] rappresentante, o sia stato esaminato in qualità di testimone o di perito;

5) qualora abbia partecipato all'adozione della decisione del tribunale di grado inferiore in relazione alla stessa questione o abbia partecipato nello stesso tribunale all'adozione di una decisione [che è stata successivamente] impugnata mediante appello o ricorso per la tutela della legalità;

6) qualora sussistano circostanze che suscitano dubbi sulla sua imparzialità.”

(2) Un giudice o un giudice popolare non può pronunciarsi sulle imputazioni (...):

(...)

3) qualora abbia [già] emesso una decisione che stabilisce che l'ammissione di colpevolezza [in questione] debba essere respinta (ai sensi dell'articolo 285.c(2)) o che debba essere respinto il patteggiamento (...).”

57. L'articolo 149.b, nel capo che disciplina le misure adottate dalla polizia nel procedimento istruttorio, all'epoca dei fatti, recitava:

“(1) Qualora sussistano motivi di sospettare (*razlogi za sum*) che un reato, il cui autore è perseguibile d'ufficio, sia stato commesso, o la cui commissione, preparazione o organizzazione siano in corso e informazioni sulle comunicazioni che utilizzano reti di comunicazione elettronica debbano essere acquisite al fine di scoprire tale reato o il suo autore, il giudice istruttore può, su motivata richiesta del pubblico ministero, ordinare all'operatore della rete di comunicazione elettronica di trasmettergli informazioni sui partecipanti, le circostanze e i fatti relativi al traffico delle comunicazioni, quali ad esempio: il numero o altro tipo di identificativo degli utenti dei servizi di comunicazione elettronica; il tipo, la data, l'ora e la durata della chiamata o del servizio di comunicazione elettronica di altro tipo; la quantità di dati inoltrati; e il luogo in cui è stato effettuato il servizio di comunicazione elettronica.

(2) La richiesta e il decreto devono avere forma scritta e devono contenere informazioni che consentano di identificare il mezzo di comunicazione elettronica, la giustificazione della motivazione, il periodo di tempo in relazione al quale sono richieste le informazioni e le altre circostanze importanti che giustificano l'applicazione della misura.

(3) Qualora sussistano motivi di sospettare che un reato, il cui autore è perseguibile d'ufficio, sia stato commesso, o la cui preparazione sia in corso, e informazioni sul proprietario o l'utente di un certo mezzo di comunicazione elettronica i cui estremi non

sono disponibili nella [pertinente] cartella, nonché informazioni sull'orario in cui il mezzo di comunicazione è stato o è utilizzato [o] debbano essere acquisite al fine di scoprire tale reato o in relazione al suo autore, la polizia può chiedere all'operatore della rete di comunicazione elettronica, con richiesta scritta e anche senza il consenso della persona cui le informazioni si riferiscono, la fornitura di tali informazioni.

(4) L'operatore della rete di comunicazione elettronica può non rivelare ai suoi clienti o a terzi che ha fornito determinate informazioni al giudice istruttore (comma primo del presente articolo) o alla polizia (articolo precedente) o l'intenzione di farlo."

58. L'articolo 285.c(1), che disciplina le udienze istruttorie, stabilisce che nel caso in cui un imputato ammetta la sua colpevolezza, il presidente del tribunale debba valutare, *inter alia*, se costui abbia effettuato l'ammissione di colpevolezza di sua spontanea volontà, se essa sia inequivoca e sia corroborata da altre prove nel fascicolo. Dopo di ciò, il presidente del tribunale emette una decisione con la quale accetta o respinge l'ammissione di colpevolezza, che non può essere impugnata (articolo 285.c(2)). In caso di accettazione dell'ammissione di colpevolezza, l'imputato non può ritirarla. La condanna è pronunciata nell'udienza di condanna. Le motivazioni della sentenza relativamente alla colpevolezza dell'imputato si limitano a constatare che quest'ultimo ha confessato i reati imputatigli e che tale confessione è stata accettata dal presidente del tribunale (articoli 285.c(3), (5) e (6), e 285.č). Ai sensi dell'articolo 330, tali disposizioni devono essere applicate, *mutatis mutandis*, all'ammissione di colpevolezza effettuata e accettata durante il processo.

59. L'articolo 324(2), concernente l'esame dell'imputato, è formulato come segue:

"(2) Quando l'imputato ha terminato la sua dichiarazione, può essere interrogato. Il presidente del tribunale invita prima il pubblico ministero poi il difensore a porre domande all'imputato. La parte lesa, il rappresentante legale, l'avvocato, il coimputato e il perito possono porre domande dirette all'imputato soltanto con il permesso del presidente del tribunale."

60. Inoltre, l'articolo 326(1) recita:

"(1) Al termine dell'interrogatorio del primo imputato, gli eventuali coimputati possono a loro volta essere interrogati. Dopo [l'interrogatorio di] ciascun [coimputato] il presidente del tribunale informa tale coimputato delle dichiarazioni rese dagli altri coimputati che sono stati interrogati prima di lui e gli chiede se abbia commenti in proposito, chiede inoltre a [ogni] imputato che è stato esaminato prima di lui se abbia commenti in merito alla dichiarazione del coimputato esaminato dopo di lui. Ogni coimputato ha diritto a porre domande a gli altri coimputati esaminati."

61. L'articolo 5(3) stabilisce che l'imputato non è obbligato a difendersi o a rispondere ad alcuna domanda; qualora decida di difendersi non può essere obbligato a rilasciare dichiarazioni che possono incriminare lui o i suoi congiunti o a confessare la propria colpevolezza.

B. Il codice penale

62. L'articolo 261 § 1 del codice penale, entrato in vigore il 1° novembre 2008, recita:

Accettazione di un compenso illecito

“(1) Il pubblico ufficiale o il funzionario pubblico che chiede o acconsente ad accettare per sé o per terzi un compenso, un dono o altra utilità, o la promessa o l'offerta di tale utilità, in cambio del compimento di un atto formale rientrante nelle funzioni del suo ufficio il cui compimento è vietato (o dell'omissione di un atto formale che deve o può essere compiuto), o che in altro modo abusa del suo ufficio, o chiunque funga da intermediario al fine di corrompere un pubblico ufficiale, è punito con la reclusione non inferiore a un anno e non superiore a otto anni e con una multa.”

63. L'articolo 54 stabilisce le condizioni affinché si possa ritenere che un reato abbia carattere continuato (ovvero sia ritenuto costituire reato continuato) e le pene che possono essere irrogate in tal caso.

C. La legge del 2004 come modificata

64. La legge in materia di comunicazioni elettroniche è rimasta in vigore dal 1° maggio 2004 al 14 gennaio 2013. Per quanto qui di pertinenza, è stata modificata nel 2006 nella parte relativa alla conservazione dei dati al fine di recepire la direttiva sulla conservazione dei dati (si veda il paragrafo 70 *infra*); è stata ulteriormente modificata nel 2009 (in prosieguo “la legge del 2004 come modificata”). Per quanto pertinente, recitava:

Articolo 104 (Dati relativi al traffico)

“(1) I dati relativi al traffico di abbonati e utenti trattati e conservati dall'operatore devono essere cancellati o resi anonimi non appena non siano più necessari per la trasmissione delle comunicazioni, eccetto che nel caso delle categorie di dati di cui all'articolo 107.b della presente legge, che devono essere conservati ai sensi dei commi 4 e 5 dell'articolo 107.a della presente legge.

(2) Fermo restando la disposizione [indicata al] precedente articolo, l'operatore può, sino al completo pagamento del servizio (ma non oltre la scadenza del termine di prescrizione), conservare e trattare i dati relativi al traffico necessari per il calcolo e il saldo delle fatture relative alle interconnessioni.

(3) Al fine della commercializzazione dei servizi di comunicazione elettronica o della fornitura di servizi a valore aggiunto, il fornitore del servizio [in questione] può trattare i dati menzionati nel primo comma del presente articolo nella misura e per la durata necessarie per siffatti servizi o commercializzazione, ma soltanto qualora l'abbonato o l'utente a cui i dati si riferiscono abbia prima prestato il proprio consenso. Gli abbonati o utenti devono essere informati (prima di prestare il consenso) dei tipi di dati relativi al traffico che sono trattati e della durata di tale trattamento. Gli abbonati o utenti hanno il diritto di ritirare il loro consenso in qualsiasi momento.

(4) Ai fini di cui al secondo comma del presente articolo, il fornitore di servizi deve indicare nei [suoi] termini e condizioni generali quali dati relativi al traffico saranno memorizzati [e] trattati e la durata di tale trattamento, e deve altresì dichiarare che i dati saranno gestiti in conformità alla legge che disciplina la protezione dei dati personali.

(5) I dati relativi al traffico possono essere trattati ai sensi dei precedenti commi del presente articolo soltanto da persone che agiscono sotto l'autorità dell'operatore e gestiscono la fatturazione o il traffico, rispondono ai quesiti dei clienti, accertano le frodi, commercializzano i servizi di comunicazione elettronica o forniscono servizi a valore aggiunto; (...) tale trattamento deve essere limitato a quanto è necessario per lo svolgimento di tali attività.

(6) Fatte salve le disposizioni di cui al primo, secondo, terzo e quinto comma del presente articolo, l'operatore invia i dati relativi al traffico all'organo competente qualora tale organo li richieda al fine della risoluzione delle controversie (in particolare di quelle attinenti all'interconnessione e alla fatturazione) in conformità alla normativa applicabile.”

Articolo 107.a
(Disposizioni generali relative ai dati conservati)

“(1) Gli operatori devono, al fine di ottenere dati sul traffico nella rete di comunicazione pubblica (come previsto dalla legge che disciplina la procedura penale) [e] al fine di garantire la sicurezza nazionale, l'ordine costituzionale e gli interessi relativi alla sicurezza, politici ed economici dello Stato (...) nonché la difesa nazionale (...) conservare i dati di cui all'articolo 107.b della presente legge qualora [tali dati] siano generati o trattati durante la fornitura dei relativi servizi pubblici di comunicazione.

(...)

(3) L'obbligo di cui al primo comma del presente articolo si applica anche alla conservazione dei dati relativi ai tentativi di chiamata non riusciti qualora tali dati siano generati, trattati, conservati o registrati all'atto della fornitura di servizi pubblici di comunicazione. Tale obbligo non si estende alla conservazione dei dati sulle connessioni fallite e al contenuto delle comunicazioni.

(...)

(5) Gli operatori assicurano la conservazione dei dati di cui al primo, terzo e quarto comma del presente articolo, in conformità alle disposizioni della presente legge, per un periodo di quattordici mesi dalla data della comunicazione (per quanto concerne i dati relativi a servizi di telefonia accessibili al pubblico) e di otto mesi dalla data della comunicazione (per quanto concerne gli altri dati).

(6) Lo (...) organo che decide in merito ai dati di cui al primo comma (...) può prorogare il periodo di conservazione per un tempo limitato qualora ciò sia richiesto da circostanze particolari inerenti all'azione penale, (...)

(7) Allo scadere del termine per la conservazione, gli operatori devono distruggere tutti i dati conservati, in conformità alle disposizioni della presente legge, eccetto quelli in relazione ai quali è stato emesso un decreto che autorizza ad accedervi o che sono già stati trasmessi all'autorità competente.”

Articolo 107.b
(I dati da conservare)

“I dati che devono essere memorizzati (in prosieguo “i dati memorizzati”) sono i seguenti:

1. i dati necessari per rintracciare, identificare e riconoscere la fonte di una comunicazione, in particolare quelli:

- concernenti la telefonia di rete fissa e la telefonia mobile: il numero telefonico del chiamante, il nome e indirizzo dell’abbonato o dell’utente registrato;

- riguardo ai [dati relativi a internet] (...);

2. i dati necessari per identificare la destinazione di una comunicazione, in particolare quelli:

- concernenti la telefonia di rete fissa e la telefonia mobile: il numero composto (...) il numero a cui è trasmessa la chiamata, [e] il nome e indirizzo dell’abbonato o dell’utente registrato;

- riguardo ai [dati relativi a internet] (...);

3. i dati necessari per determinare la data, l’ora e la durata di una comunicazione, in particolare quelli:

- concernenti la telefonia di rete fissa e la telefonia mobile: data e ora dell’inizio della comunicazione e la durata o l’orario della fine della comunicazione;

- riguardo ai [dati relativi a internet] (...);

4. i dati necessari per determinare il tipo di comunicazione, in particolare quelli:

- concernenti la telefonia di rete fissa e la telefonia mobile: il servizio telefonico utilizzato;

- riguardo ai [dati relativi a internet] (...);

5. i dati necessari per identificare le apparecchiature di comunicazione degli utenti, in particolare quelli:

- concernenti la telefonia di rete fissa: il numero dal quale è stata effettuata la chiamata e il numero chiamato;

- concernenti la telefonia mobile: i numeri telefonici chiamanti e chiamati; l’identità utente mobile internazionale [*International Mobile Subscriber Identity:IMSI*] del chiamante e del chiamato, il codice IMEI [*International Mobile Equipment Identity*] del chiamante e del chiamato, [e] | nel caso dei servizi prepagati anonimi, la data e l’ora dell’attivazione iniziale del servizio e l’etichetta di ubicazione [ovvero la *cell ID*] dalla quale è stato fornito il servizio;

- riguardo ai [dati relativi a internet] (...);

6. i dati necessari per determinare l’ubicazione dell’apparecchiatura di comunicazione mobile [in questione]:

- l’etichetta di ubicazione (*cell ID*) all’inizio della comunicazione;

- i dati per identificare l'ubicazione geografica delle cellule facendo riferimento alle loro etichette di ubicazione nel periodo in cui vengono conservati i dati relativi alle comunicazioni.”

Articolo 107.c
(Protezione dei dati conservati)

“(1) Gli operatori garantiscono la tutela dei dati conservati in conformità alla legge che disciplina la protezione dei dati personali. A tal fine adottano, singolarmente o congiuntamente, misure tecniche e organizzative idonee a proteggere i dati conservati dalla distruzione, perdita o alterazione e dalle forme non autorizzate o illecite di memorizzazione, trattamento, accesso o divulgazione.

(2) Gli operatori possono trattare i dati conservati soltanto nella misura necessaria ad assicurare la loro memorizzazione.

(3) I dati conservati sono della stessa qualità di quelli in rete. I dati conservati sono soggetti alle disposizioni della presente legge che riguardano la protezione e la salvaguardia dei dati in rete.

(4) L'agenzia [della posta e delle comunicazioni elettroniche], dopo aver acquisito il parere del Commissario all'informazione, stabilisce in dettaglio in un regolamento generale le modalità di memorizzazione dei dati e il metodo di applicazione del presente articolo.”

Articolo 107.č
(Decreto che autorizza l'accesso e la trasmissione dei dati)

“(1) L'operatore trasmette i dati conservati immediatamente o al più tardi entro tre giorni dalla ricezione della copia della parte del decreto dell'autorità competente che indica tutte le informazioni necessarie relative alla portata dell'accesso.

(...)

(3) All'atto della ricezione del decreto l'operatore trasmette i dati conservati all'autorità competente nella misura specificata nella copia del dispositivo del decreto.

(4) Gli operatori, congiuntamente a [le] autorità che possono chiedere l'accesso ai dati conservati, garantiscono la sussistenza, per un periodo di dieci anni, di una documentazione indelebile di ciascuna trasmissione dei dati conservati e, entro tale periodo, memorizzano i dati ottenuti e forniti a decorrere dalla data della loro trasmissione all'autorità competente, proteggendoli in conformità (...) alla qualifica di riservatezza indicata nel decreto.

(5) Il ministro, di concerto con il ministro dell'interno, il ministro della difesa e il direttore dell'Agenzia slovena di intelligence e sicurezza stabilisce in dettaglio le modalità di trasmissione dei dati conservati.”

**Articolo 112
(Vigilanza)**

“(..)

(2) Il Commissario all’informazione vigila sulla memorizzazione dei dati relativi al traffico e all’ubicazione ottenuti o trattati in relazione alla necessità di garantire reti o servizi pubblici di comunicazione, in conformità agli articoli 107.a-e della presente legge e sulla trasmissione di dati di cui all’articolo 104.a della presente legge.”

**Articolo 142
(Collaborazione tra le autorità di controllo)**

“L’agenzia, gli (...) ispettori e il Commissario all’informazione hanno il dovere di collaborare e informarsi reciprocamente delle misure di controllo adottate, di fornirsi vicendevolmente le informazioni necessarie all’attuazione della vigilanza e di collaborare dal punto di vista professionale.”

65. Nel 2012 la legge del 2004 come modificata è stata sostituita da una nuova legge (ovvero “la legge del 2012”) i cui articoli 163 e 164 contengono le stesse disposizioni contenute negli articoli 107.a e 107.b della legge del 2004 come modificata.

D. La decisione della Corte costituzionale U-I-65/13 del 3 luglio 2014

66. Su richiesta del Commissario sloveno all’informazione, la Corte costituzionale aveva esaminato la costituzionalità della legge del 2012 in relazione alla conservazione dei dati, in particolare dei suoi articoli 163 e 164 (si veda il paragrafo 65 *supra*). Con decisione del 3 luglio 2014, la Corte costituzionale, rinviando alla sentenza della CGUE in data 8 aprile 2014 (*Digital Rights Ireland e altri*– si vedano i paragrafi 74-76 *infra*) aveva annullato le relative disposizioni della legge del 2012 ritenendole non conformi al diritto alla protezione dei dati personali.

67. La Corte costituzionale aveva ritenuto che il trattamento dei dati personali ai sensi delle disposizioni impugnate costituisse un’ingerenza nel diritto alla protezione dei dati personali (articolo 38 § 1 della Costituzione). Aveva stabilito inoltre che le finalità perseguite dal legislatore, ovvero, *inter alia*, la prevenzione, le indagini e il perseguimento dei reati gravi, erano leciti. A suo giudizio, anche i mezzi utilizzati erano idonei al conseguimento di tali finalità. In ordine alla necessità dell’ingerenza, la Corte costituzionale aveva osservato, *inter alia*, che la conservazione obbligatoria e non selettiva dei dati relativi al traffico interferiva nei diritti di molte persone che non erano - né mai lo sarebbero in alcun modo state - collegate alle finalità per le quali i dati erano raccolti. In particolare, la legislazione in questione non limitava la conservazione dei dati a un certo periodo di tempo, a una certa area geografica o a una cerchia di persone che potevano avere un qualche legame con le finalità perseguite dalla misura. Il legislatore inoltre non aveva giustificato il

motivo per il quale era necessaria la durata stabilita della conservazione dei dati in questione (quattordici, o, in alcuni casi, otto mesi); in più non aveva specificato i reati che giustificavano la conservazione dei dati.

68. Rilevando la gravità dell'ingerenza e ritenendo che il legislatore non avesse limitato il campo di applicazione della misura a quanto necessario per ottenere gli obiettivi perseguiti, la Corte costituzionale aveva concluso che le disposizioni impugnate costituivano un'ingerenza sproporzionata nel diritto alla protezione dei dati personali ed erano incostituzionali. Le aveva annullate disponendo l'immediata distruzione dei dati conservati in virtù di tali disposizioni. Il 10 novembre 2022 è entrata in vigore una nuova legge in materia di comunicazioni elettroniche. Non prevede la conservazione generalizzata dei dati relativi alle telecomunicazioni per scopi diversi da quelli relativi alla fornitura di servizi commerciali.

II. IL DIRITTO E LA PRASSI DELL'UNIONE EUROPEA IN MATERIA DI PROTEZIONE DEI DATI E PRIVACY

A. Il pertinente diritto della UE

69. Gli articoli 7, 8 e 11 della Carta dei diritti fondamentali dell'Unione europea ("la Carta") recitano:

Articolo 7 – Rispetto della vita privata e della vita familiare

"Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni."

Articolo 8 – Protezione dei dati di carattere personale

"1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente."

Articolo 11 – Libertà di espressione e d'informazione

"1. Ogni persona ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa esservi ingerenza da parte delle autorità pubbliche e senza limiti di frontiera.

2. La libertà dei media e il loro pluralismo sono rispettati."

70. Le disposizioni di legge interne in materia di conservazione dei dati (si vedano i paragrafi 64-65 *supra*), oggetto delle doglianze del ricorrente hanno recepito la 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/CE (GU 2006 L 105, p. 54) (in prosieguo "la direttiva sulla conservazione dei dati"). Tale direttiva stabilisce l'obbligo per i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione di conservare alcuni dati che sono stati da loro generati o trattati per garantire la loro disponibilità a fini di indagine, accertamento e perseguimento dei reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale. La direttiva sulla conservazione dei dati si applica ai dati relativi al traffico e all'ubicazione e ai dati connessi necessari per identificare l'abbonato o l'utente registrato in questione. Non si applica al contenuto delle comunicazioni elettroniche (articolo 1). L'articolo 3 stabilisce l'obbligo di conservazione dei dati specificati all'articolo 5 (recepito dall'articolo 107.b della legge del 2004 come modificata, si veda il paragrafo 64 *supra*). L'articolo 6 stabilisce che tali dati siano conservate per periodi non inferiori a sei mesi e non superiori a due anni dalla data della comunicazione in questione. Ai sensi dell'articolo 8 della direttiva sulla conservazione dei dati gli Stati membri devono garantire che tali dati siano conservati in modo tale che essi (e ogni altra informazione necessaria ad essi collegata) possano essere trasmessi immediatamente alle autorità competenti su loro richiesta.

71. La direttiva relativa alla vita privata e alle comunicazioni elettroniche (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 (la direttiva e-privacy), consolidata nella versione testuale del 19 dicembre 2009, che combina la legge iniziale e le successive modifiche ad essa apportate dalla direttiva 2009/136/CE del 25 novembre 2009 e dalla sua rettifica 2009/136 del 10 settembre 2013) contiene disposizioni specifiche destinate a offrire agli utenti di servizi di comunicazione elettronica protezione dai rischi per i loro dati personali e la loro vita privata derivanti dalle nuove tecnologie e dall'accresciuta capacità di memorizzazione e trattamento dei dati (considerando 5-7 di tale direttiva). L'articolo 5 (1) stabilisce che gli Stati membri assicurino la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati al traffico. Stabilisce inoltre il divieto per tutte le persone diverse dagli utenti, *inter alia*, di memorizzare, senza consenso di questi ultimi, i dati sul traffico relativi alle comunicazioni elettroniche, eccetto quando ciò sia autorizzato legalmente a norma dell'articolo 15 (1). Quest'ultima disposizione stabilisce le condizioni che

permettono di derogare al principio di riservatezza consentendo agli Stati membri di adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, (1), (2), (3) e 4), e all'articolo 9 di tale direttiva, qualora tale restrizione costituisca 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. Stabilisce che a tal fine gli Stati membri possano tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per motivi specificati e che tali misure siano conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, § 1 e 2, del trattato sull'Unione europea.

72. Ai sensi dell'articolo 6 della direttiva e-privacy i dati sul traffico relativi agli abbonati e agli utenti trattati e memorizzati dal fornitore di una rete pubblica di comunicazione o di un servizio di comunicazione elettronica accessibile al pubblico, devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione. Inoltre il trattamento dei dati sul traffico è consentito, a determinate condizioni, a fini di fatturazione e di commercializzazione dei servizi o per la fornitura di servizi a valore aggiunto. Per quanto riguarda la fatturazione dei servizi tale trattamento è consentito solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o instaurato un procedimento giudiziario per pretendere il pagamento. Per quanto riguarda i dati relativi all'ubicazione diversi dai dati relativi al traffico, l'articolo 9 § 1 di tale direttiva stabilisce che essi possano essere sottoposti a trattamento soltanto a determinate condizioni e 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.

73. In ordine alla direttiva generale sulla protezione dei dati e alla direttiva polizia (*Law-Enforcement Directive LED*) si veda *Ekimdzhiev e altri c. Bulgaria*, n. 70078/12, §§ 234-39, 11 gennaio 2022.

B. La pertinente giurisprudenza della Corte di giustizia dell'Unione europea

1. Digital Rights Ireland e altri (C-293/12 e C-594/12, EU:C:2014:238)

74. A seguito di una domanda di pronuncia pregiudiziale (che trae origine da un'azione promossa dalla società irlandese Digital Rights Ireland dinanzi alla *High Court* irlandese e da diversi ricorsi costituzionali promossi dinanzi alla Corte costituzionale austriaca), la CGUE ha valutato la validità della direttiva sulla conservazione dei dati, in particolare alla luce degli articoli 7 e 8 della Carta. In data 8 aprile 2014 (si veda il paragrafo 66 *supra* per il

riferimento completo) tale corte ha dichiarato invalida la direttiva sulla conservazione dei dati.

75. La CGUE ha osservato che i dati che i fornitori di servizi di comunicazione erano obbligati a conservare in virtù della direttiva sulla conservazione dei dati, presi nel loro complesso potevano permettere di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati erano stati conservati. I seguenti passi sono particolarmente rilevanti sotto questo profilo:

“26 in proposito, va rilevato che i dati che i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione debbono conservare, ai sensi degli articoli 3 e 5 della direttiva 2006/24, sono, in particolare, i dati necessari per rintracciare e identificare la fonte di una comunicazione e la destinazione della stessa, per stabilire la data, l'ora, la durata e il tipo di una comunicazione, le attrezzature di comunicazione degli utenti nonché per determinare l'ubicazione delle apparecchiature di comunicazione mobile, dati tra i quali figurano, segnatamente, il nome e l'indirizzo dell'abbonato o dell'utente registrato, il numero telefonico chiamante e quello chiamato, nonché un indirizzo IP per i servizi Internet. I suddetti dati permettono, in particolare, di sapere quale sia la persona con cui un abbonato o un utente registrato ha comunicato e con quale mezzo, così come di stabilire il tempo della comunicazione e il luogo dal quale questa è avvenuta. Inoltre, essi permettono di conoscere la frequenza delle comunicazioni dell'abbonato o dell'utente registrato con talune persone nel corso di un determinato periodo.

27 Questi dati, presi nel loro complesso, possono permettere di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati.”

La CGUE ha ritenuto inoltre che prevedendo la conservazione e il trattamento dei dati personali la direttiva sulla conservazione dei dati costituisse un'ingerenza nei diritti garantiti dagli articoli 7 e 8 della Carta di vasta portata e di particolare gravità. Facendo riferimento alle cause *Leander c. Svezia* (26 marzo 1987, § 48, serie A n 116), *Rotaru c. Romania* ([GC], n. 28341/95, § 46, CEDU 2000-V), e *Weber e Saravia c. Germania* ((dec.), n. 54934/00, § 79, CEDU 2006-XI), la CGUE ha osservato che l'accesso da parte delle autorità nazionali competenti a tali dati costituiva un'ingerenza supplementare nei diritti tutelati dall'articolo 7 della Carta. Ha rilevato che il fatto che la conservazione dei dati e l'utilizzo ulteriore degli stessi fossero effettuati senza che l'abbonato o l'utente registrato ne fossero informati poteva ingenerare nelle persone interessate la sensazione che la loro vita privata fosse oggetto di costante sorveglianza.

76. In ordine alla giustificazione dell'ingerenza, la CGUE ha osservato che la direttiva impugnata non permetteva di venire a conoscenza del contenuto delle comunicazioni elettroniche in quanto tale ed esigeva che la conservazione dei dati fosse accompagnata da alcune misure di sicurezza. L'ingerenza pertanto non pregiudicava la sostanza dei diritti garantiti dagli articoli 7 e 8 della Carta. Dopo aver constatato che la conservazione dei dati

per permettere alle autorità nazionali competenti di disporre di un accesso eventuale agli stessi rispondeva effettivamente a un obiettivo di interesse generale (ovvero la lotta contro i reati gravi), la CGUE era passata a esaminare la proporzionalità dell'ingerenza, pervenendo in proposito, *inter alia*, alle seguenti conclusioni:

“49 Per quel che riguarda la questione consistente nell'accertare se la conservazione dei dati sia idonea a realizzare l'obiettivo perseguito dalla direttiva 2006/24, si deve constatare che, tenuto conto della crescente importanza dei mezzi di comunicazione elettronica, i dati che debbono essere conservati in attuazione della detta direttiva permettono alle autorità nazionali competenti in materia di perseguimento di reati di disporre di possibilità supplementari di accertamento dei reati gravi e, al riguardo, costituiscono quindi uno strumento utile per le indagini penali. Pertanto, la conservazione dei suddetti dati può essere considerata come idonea a realizzare l'obiettivo perseguito dalla suddetta direttiva.

(...)

54 Pertanto, la normativa dell'Unione di cui trattasi deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura di qua e impongano requisiti minimi in modo che le persone i cui dati sono stati conservati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati (v., per analogia, per quanto riguarda l'articolo 8 della CEDU, sentenze Corte EDU., *Liberty e altri c. Regno Unito*, 1° luglio 2008, n. 58243/00, § 62 63; *Rotaru c. Romania*, § da 57 a 59, e *S. e Marper c. Regno Unito*, § 99).

55 La necessità di disporre di siffatte garanzie è tanto più importante allorché, come prevede la direttiva 2006/24, i dati personali sono soggetti a trattamento automatico ed esiste un rischio considerevole di accesso illecito ai dati stessi (v., per analogia, con riguardo all'articolo 8 della CEDU, sentenze Corte EDU., *S. e Marper c. Regno Unito*, § 103, e *M. K. c. Francia*, 18 aprile 2013, n. 19522/09, § 35).

(...)

57 A questo proposito, si deve rilevare, in primo luogo, che la direttiva 2006/24 riguarda in maniera generale qualsiasi persona e qualsiasi mezzo di comunicazione elettronica nonché l'insieme dei dati relativi al traffico senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi.

58 Infatti, da un lato, la direttiva 2006/24 riguarda in maniera globale l'insieme delle persone che fanno uso dei mezzi di comunicazione elettronica, senza tuttavia che le persone i cui dati vengono conservati debbano trovarsi, anche indirettamente, in una situazione che possa dar luogo a indagini penali. Essa pertanto si applica anche a persone per le quali non esiste alcun indizio tale da far credere che il loro comportamento possa avere un nesso, ancorché

indiretto o lontano, con reati gravi. Inoltre, essa non prevede alcuna deroga, e pertanto si applica anche a persone le cui comunicazioni sono soggette, in base alle norme del diritto nazionale, al segreto professionale.

59 Dall'altro lato, pur mirando a contribuire alla lotta contro la criminalità grave, la suddetta direttiva non impone alcuna relazione tra i dati di cui prevede la conservazione e una minaccia per la sicurezza pubblica e, in particolare, non limita la conservazione dei dati a quelli relativi a un determinato periodo di tempo e/o a un'area geografica determinata e/o a una cerchia di persone determinate che possano essere coinvolte, in un modo o nell'altro, in un reato grave, né alle persone la conservazione dei cui dati per altri motivi, potrebbe contribuire alla prevenzione, all'accertamento o al perseguimento di reati gravi.

60 In secondo luogo, alla suddetta mancanza generale di limiti si aggiunge il fatto che la direttiva 2006/24 non prevede alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore a fini di prevenzione, di accertamento o di indagini penali riguardanti reati che possano, con riguardo alla portata e alla gravità dell'ingerenza nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta, essere considerati sufficientemente gravi da giustificare siffatta ingerenza. Al contrario, la direttiva 2006/24 si limita a rinviare, all'articolo 1, paragrafo 1, in maniera generale ai reati gravi come definiti da ciascuno Stato membro nel proprio diritto interno.

61 Inoltre, per quanto riguarda l'accesso delle autorità nazionali competenti ai dati e al loro uso ulteriore, la direttiva 2006/24 non contiene le condizioni sostanziali e procedurali ad esso relative. (...)

62 In particolare, la direttiva 2006/24 non prevede alcun criterio oggettivo che permetta di limitare il numero di persone che dispongono dell'autorizzazione di accesso e di uso ulteriore dei dati conservati a quanto strettamente necessario alla luce dell'obiettivo perseguito. Soprattutto, l'accesso ai dati conservati da parte delle autorità nazionali competenti non è subordinato ad un previo controllo effettuato da un giudice o da un'entità amministrativa indipendente la cui decisione sia diretta a limitare l'accesso ai dati e il loro uso a quanto strettamente necessario per raggiungere l'obiettivo perseguito e intervenga a seguito di una richiesta motivata delle suddette autorità presentata nell'ambito di procedure di prevenzione, di accertamento o di indagini penali. Non è neppure stato previsto un obbligo preciso degli Stati membri volto a stabilire simili limitazioni.

63 In terzo luogo, quanto alla durata di conservazione dei dati, la direttiva 2006/24 impone, all'articolo 6, la conservazione degli stessi per un periodo di almeno sei mesi senza che venga effettuata alcuna distinzione tra le categorie di dati previste all'articolo 5 della direttiva a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda delle persone interessate.

64 Tale durata, inoltre, si colloca tra un minimo di sei mesi e un massimo di ventiquattro mesi, senza che venga precisato che la determinazione della durata

di conservazione debba basarsi su criteri obiettivi al fine di garantire che sia limitata allo stretto necessario.

65 Da quanto precede deriva che la direttiva 2006/24 non prevede norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta. Pertanto, è gioco forza constatare che tale direttiva comporta un'ingerenza nei suddetti diritti fondamentali di vasta portata e di particolare gravità nell'ordinamento giuridico dell'Unione, senza che siffatta ingerenza sia regolamentata con precisione da disposizioni che permettano di garantire che essa sia effettivamente limitata a quanto strettamente necessario.

66 Per di più, per quanto riguarda le norme riguardanti la sicurezza e la protezione dei dati conservati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, si deve constatare che la direttiva 2006/24 non prevede garanzie sufficienti, come richieste dall'articolo 8 della Carta, che permettano di assicurare una protezione efficace dei dati conservati contro i rischi di abuso nonché contro eventuali accessi e usi illeciti dei suddetti dati. (...)

(...)

69 Alla luce dell'insieme delle osservazioni che precedono, si deve considerare che, adottando la direttiva 2006/24, il legislatore dell'Unione ha ecceduto i limiti imposti dal rispetto del principio di proporzionalità alla luce degli articoli 7, 8 e 52, paragrafo 1, della Carta.”

2. Tele2 Sverige e Watson e altri (C-203/15 e C-698/15, EU:C:2016:970)

77. Nella sentenza del 21 dicembre 2016 (emessa a seguito di domande di rinvio pregiudiziale proposte dalla Corte di appello amministrativa di Stoccolma, Svezia, e dalla Corte di appello di Inghilterra e Galles) i giudici del rinvio avevano sollevato, *inter alia*, la questione se un obbligo generalizzato e indifferenziato di conservazione dei dati relativi alle comunicazioni elettroniche fosse *per se* incompatibile con gli articoli 7 e 8 e l'articolo 52 § 1, della Carta o se la compatibilità di una siffatta conservazione di dati dovesse essere valutata alla luce delle norme disciplinanti l'accesso ai dati, la protezione di questi ultimi e la loro sicurezza, nonché la durata della loro conservazione. La CGUE ha chiarito che, pur potendo gli Stati membri adottare (conformemente all'articolo 15 § 1 della direttiva e-privacy) misure legislative che prevedono la conservazione dei dati relativi al traffico e all'ubicazione, tale conservazione doveva costituire un'eccezione e non la regola. A tale proposito, ha ritenuto che l'articolo 15 § 1, di tale direttiva, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, non ostasse a che uno Stato membro adottasse una normativa la quale consentisse (a titolo preventivo) la conservazione mirata dei dati relativi al traffico e all'ubicazione, per finalità di lotta contro la criminalità grave;

tuttavia tale conservazione dei dati, per quanto riguardava le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone riguardate, nonché la durata di conservazione prevista, era limitata allo stretto necessario. In particolare, la conservazione dei dati doveva rispondere a criteri oggettivi che istituivano un rapporto tra i dati da conservare e l'obiettivo perseguito. Tali condizioni dovevano risultare, in pratica, idonee a delimitare effettivamente la portata della misura e, di conseguenza, il pubblico interessato. La CGUE ha poi osservato:

“111 (...) Per quanto riguarda la delimitazione di una misura siffatta sotto il profilo del pubblico e delle situazioni potenzialmente riguardati, la normativa nazionale deve essere fondata su elementi oggettivi, che permettano di prendere in considerazione un pubblico i cui dati sono idonei a rivelare una connessione, almeno indiretta, con atti di criminalità grave, a contribuire in un modo o in un altro alla lotta contro la criminalità grave, o a prevenire un grave rischio per la sicurezza pubblica. Una siffatta delimitazione può essere ottenuta mediante un criterio geografico qualora le autorità nazionali competenti considerino, sulla base di elementi oggettivi, che esiste, in una o più zone geografiche, un rischio elevato di preparazione o di commissione di atti di questo tipo.”

3. *La Quadrature du Net e altri (C-511/18, C-512/18 e C-520/18, EU:C:2020:791)*

78. Nella sentenza del 6 ottobre 2020, pronunciata a seguito delle domande di rinvio pregiudiziale proposte dal Consiglio di Stato francese e dalla Corte costituzionale belga, la CGUE ha rinviato, *inter alia*, alle conclusioni delle summenzionate sentenze e ha chiarito che la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione costituiva, di per sé, da un lato, una deroga al divieto, previsto dall'articolo 5 § 1, della direttiva e-privacy e, dall'altro, un'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta, a prescindere dalla circostanza che le informazioni relative alla vita privata di cui trattasi avessero o meno un carattere sensibile o che gli interessati avessero o meno subito eventuali inconvenienti in seguito a siffatta ingerenza. Ha osservato inoltre che sotto questo profilo era irrilevante la circostanza che i dati conservati fossero stati o meno utilizzati successivamente. Nella sentenza del 6 ottobre 2020 la CGUE ha specificamente trattato l'obiettivo della salvaguardia della sicurezza nazionale constatando che la sua importanza superava quella degli altri obiettivi di cui all'articolo 15 § 1, della direttiva 2002/58, che poteva giustificare una misura legislativa che autorizzava le autorità competenti ad imporre ai fornitori di servizi di comunicazione elettronica di procedere alla conservazione dei dati relativi al traffico e all'ubicazione di tutti gli utenti dei servizi di comunicazione elettronica per un periodo limitato, se ricorrevano circostanze sufficientemente concrete che consentivano di ritenere che lo Stato membro interessato si trovasse di fronte a una grave minaccia alla

sicurezza nazionale, che la CGUE specificava ulteriormente e che doveva rivelarsi reale e attuale o prevedibile. Tuttavia anche la conservazione di tale tipo non poteva avere carattere sistematico e doveva essere oggetto di un controllo da parte di un giudice o di un organo amministrativo indipendente.

79. La CGUE ha ritenuto inoltre che non fosse precluso agli Stati membri adottare misure legislative a fini di lotta alle forme gravi di criminalità (e, *a fortiori*, di salvaguardia della sicurezza nazionale) facendo ricorso a un'ingiunzione che imponesse ai fornitori di servizi di comunicazione elettronica (mediante un provvedimento dell'autorità competente soggetto a un controllo giurisdizionale effettivo) di procedere, per un periodo determinato, alla conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione di cui detti fornitori di servizi dispongono. Ha osservato che al fine di garantire che l'ingerenza che una misura di questo tipo costituisce sia limitata allo stretto necessario, occorre (i) che l'obbligo di conservazione riguardi unicamente i dati relativi al traffico e i dati relativi all'ubicazione che possono contribuire all'accertamento di reati gravi o di attentati alla sicurezza nazionale, e (ii) che la durata di conservazione dei dati sia limitata allo stretto necessario, potendo tuttavia essere prorogata quando le circostanze e l'obiettivo perseguito da detta misura lo giustificano. Ha osservato inoltre che una siffatta conservazione rapida non doveva essere limitata ai dati delle persone concretamente sospettate di avere commesso un reato o un attentato alla sicurezza nazionale; poteva invece essere estesa ai dati relativi al traffico e ai dati relativi all'ubicazione afferenti a persone diverse da quelle sospettate di avere progettato o commesso un reato grave o un attentato alla sicurezza nazionale, purché tali dati potessero contribuire, sulla base di elementi oggettivi e non discriminatori, all'accertamento di un siffatto reato o attentato alla sicurezza nazionale.

80. In ordine alla limitazione nel tempo degli effetti di una dichiarazione di illegittimità riguardante la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione e l'utilizzo nell'ambito di un procedimento penale di elementi di prova che sono stati ottenuti mediante tale conservazione, la CGUE ha concluso:

“228 (...) Un giudice nazionale non può applicare una disposizione del suo diritto nazionale che lo autorizzi a limitare nel tempo gli effetti di una dichiarazione di illegittimità ad esso incombente, in forza di tale diritto, nei confronti di una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica, a fini, in particolare, di salvaguardia della sicurezza nazionale e di lotta alla criminalità, una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione incompatibile con l'articolo 15, § 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, § 1, della Carta. Detto articolo 15 § 1, interpretato alla luce del principio di effettività, impone al giudice penale nazionale di non tenere conto delle informazioni e degli elementi di prova ottenuti mediante una conservazione generalizzata e indifferenziata dei dati

relativi al traffico e dei dati relativi all'ubicazione incompatibile con il diritto dell'Unione, nell'ambito di un procedimento penale avviato nei confronti di persone sospettate della commissione di reati, qualora dette persone non siano in grado di prendere efficacemente posizione su tali informazioni ed elementi di prova, che provengono da un settore che esula dalla competenza dei giudici e che possono influenzare in modo preponderante la valutazione dei fatti.”

81. In ordine all'ammissibilità delle prove la CGUE ha ribadito che allo stato attuale del diritto dell'Unione, spetta, in linea di principio, esclusivamente al diritto nazionale determinare le norme relative all'ammissibilità e alla valutazione, nell'ambito di un procedimento penale avviato nei confronti di persone sospettate della commissione di reati gravi, di informazioni ed elementi di prova ottenuti mediante una siffatta conservazione di dati contraria al diritto dell'Unione.

4. *Prokuratuur (C-746/18, EU:C:2021:152)*

82. La sentenza del 2 marzo 2021, pronunciata a seguito di una domanda di rinvio pregiudiziale proposta dalla Corte suprema dell'Estonia trae origine da un procedimento nel quale H.K. era stato dichiarato colpevole, *inter alia*, di diversi furti sulla base, *inter alia*, di elementi di prova ottenuti da un fornitore di servizi di comunicazione. L'autorità inquirente, dopo la concessione da parte della procura competente di diverse autorizzazioni a tal fine, aveva acquisito i dati relativi al traffico e all'ubicazione riguardanti i numeri telefonici e i codici IMEI di H.K. (che erano stati conservati per un periodo di un anno da detti fornitori) nel procedimento istruttorio. La CGUE ha ribadito che l'articolo 15 § 1 della direttiva e-privacy consente l'accesso ai dati relativi al traffico e all'ubicazione conservati a fini di lotta ai reati, soltanto quando il reato in questione è grave o rappresenta una grave minaccia alla sicurezza pubblica. La CGUE ha osservato inoltre che l'articolo 15 § 1 si applica indipendentemente dalla durata del periodo per il quale l'accesso viene richiesto, nonché dalla quantità e dalla natura dei dati disponibili per tale periodo. In ordine all'ammissibilità degli elementi di prova la CGUE, rinviando alla sentenza *Quadrature du Net e altri*, ha osservato:

“44 La necessità di escludere informazioni ed elementi di prova ottenuti in violazione delle prescrizioni del diritto dell'Unione deve essere valutata alla luce, in particolare, del rischio che l'ammissibilità di informazioni ed elementi di prova siffatti comporta per il rispetto del principio del contraddittorio e, pertanto, del diritto ad un processo equo. Orbene, un organo giurisdizionale, il quale consideri che una parte non è in grado di svolgere efficacemente le proprie osservazioni in merito a un mezzo di prova rientrante in una materia estranea alla conoscenza dei giudici e idoneo ad influire in modo preponderante sulla valutazione dei fatti, deve constatare una violazione del diritto ad un processo equo ed escludere tale mezzo di prova al fine di evitare una violazione siffatta. Pertanto, il principio di effettività impone al giudice penale nazionale di

escludere informazioni ed elementi di prova che siano stati ottenuti mediante una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione incompatibile con il diritto dell'Unione, o anche mediante un accesso dell'autorità competente a tali dati in violazione del diritto dell'Unione, nell'ambito di un procedimento penale instaurato nei confronti di persone sospettate di atti di criminalità, qualora tali persone non siano in grado di svolgere efficacemente le proprie osservazioni in merito alle informazioni e agli elementi di prova suddetti, riconducibili ad una materia estranea alla conoscenza dei giudici e idonei ad influire in maniera preponderante sulla valutazione dei fatti (v., in tal senso, 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 226 e 227)."

83. La CGUE ha poi ritenuto che non si potesse attribuire il potere di esaminare le richieste di autorizzazione all'accesso alla procura, giacché il suo ruolo di direzione del procedimento istruttorio e dell'azione penale condizionava la sua indipendenza rispetto alle parti di un procedimento penale.

5. *Commissioner of An Garda Síochána e altri (C-140/20, EU:C:2022:258)*

84. La sentenza del 5 aprile 2022 è stata pronunciata a seguito di una richiesta di rinvio pregiudiziale proposta dalla Corte suprema dell'Irlanda. Concerneva il procedimento nel quale G.D., che era stato condannato per omicidio, chiedeva una declaratoria di invalidità di alcune disposizioni del diritto interno (ovvero quelle che prevedevano la conservazione dei dati relativi al traffico e all'ubicazione e consentivano la loro divulgazione qualora fossero necessari, *inter alia*, alla prevenzione, all'accertamento, alle indagini o al perseguimento di un reato grave) al fine di contestare l'ammissibilità di tali prove nel procedimento penale. La CGUE ha osservato che la criminalità, anche particolarmente grave, non poteva essere equiparata a una minaccia per la sicurezza nazionale. I dati relativi al traffico e i dati relativi all'ubicazione non potevano quindi essere oggetto di una conservazione generalizzata e indifferenziata ai fini della lotta alla criminalità grave e, pertanto, l'accesso a tali dati non poteva essere giustificato a questi stessi fini. Ha ribadito che è consentita soltanto la conservazione mirata dei dati relativi al traffico e all'ubicazione e la loro conservazione rapida alle condizioni indicate nella sentenza *La Quadrature du Net e altri* (paragrafi 78-80 *supra*). Ha spiegato che gli Stati membri avevano la facoltà di adottare misure di conservazione nei confronti di persone che, in base all'identificazione, risultavano (i) sottoposte ad indagine o ad altre misure di sorveglianza o (ii) iscritte nel casellario giudiziario nazionale in quanto condannate per un reato grave comportante un elevato rischio di recidiva; la CGUE ha aggiunto che quando l'identificazione era fondata su elementi oggettivi e non discriminatori, definiti dal diritto nazionale, la conservazione mirata riguardante persone così identificate era giustificata. Ha spiegato

inoltre che non era precluso alle autorità nazionali competenti disporre una misura di conservazione rapida fin dalla prima fase dell'indagine relativa a una minaccia grave per la sicurezza pubblica o a un eventuale atto di criminalità grave, ossia dal momento in cui tali autorità, secondo le pertinenti disposizioni del diritto nazionale, potevano avviare una siffatta indagine.

85. In ordine all'accesso delle autorità competenti ai dati relativi al traffico e all'ubicazione conservati, la CGUE ha ribadito che tale accesso era subordinato al controllo preventivo di un giudice o di un organo amministrativo indipendente e che la decisione di tale giudice o di tale organo doveva intervenire a seguito di una richiesta motivata di tali autorità presentata, in particolare, nell'ambito di procedure di prevenzione, di accertamento o di azione penale. La CGUE ha constatato che il funzionario di polizia dell'ordinamento giuridico in esame, che era stato autorizzato a svolgere un controllo preventivo delle richieste di accesso ai dati, non aveva soddisfatto i requisiti di indipendenza e imparzialità.

86. In ordine all'effetto dell'interpretazione della direttiva e-privacy e della Carta confermata nelle sue precedenti sentenze *Tele2 Sverige e Watson e altri* e *La Quadrature du Net e altri*, la CGUE ha ribadito che, secondo giurisprudenza costante, l'interpretazione che la Corte dà di una norma di diritto dell'Unione, nell'esercizio della competenza attribuitale dall'articolo 267 del Trattato europeo sul funzionamento dell'Unione europea, chiarisce e precisa il significato e la portata di tale norma, come deve o avrebbe dovuto essere intesa ed applicata dal momento della sua entrata in vigore. Secondo la CGUE la norma così interpretata può e deve essere applicata dal giudice anche a rapporti giuridici sorti e costituiti prima della pronuncia della sentenza che statuisce sulla domanda di interpretazione, purché sussistano i presupposti per sottoporre al giudice competente una controversia relativa all'applicazione di detta norma. In ordine all'ammissione delle prove dedotte contro G.D. la CGUE ha fatto riferimento al principio dell'autonomia procedurale degli Stati membri della UE e ai principi indicati nella sentenza *Prokuratuur*.

6. *SpaceNet e Telekom Deutschland (C-793/19 e C-794/19, EU:C:2022:702)*

87. Infine, la sentenza del 20 settembre 2022, pronunciata a seguito della richiesta di rinvio pregiudiziale proposta dalla Corte amministrativa federale tedesca, concernente la questione se agli Stati membri fosse precluso adottare una misura legislativa nazionale che, salvo talune eccezioni, imponeva ai fornitori di servizi di comunicazione elettronica, ai fini elencati all'articolo 15 §1, della direttiva e-privacy, e in particolare ai fini del perseguimento dei reati gravi o della prevenzione di un rischio concreto per la sicurezza nazionale, la conservazione generalizzata e indiscriminata di gran parte dei dati relativi al traffico e dei dati relativi all'ubicazione degli utenti finali di tali servizi, prevedendo un periodo di conservazione di varie settimane

nonché norme volte a garantire un'efficace protezione dei dati conservati dai rischi di abuso e da qualsiasi accesso illecito a tali dati. La CGUE ha ritenuto che non si potesse considerare l'obbligo di conservazione dei dati in esame conservazione mirata e che il periodo di conservazione dei dati relativi al traffico (dieci settimane) e all'ubicazione (quattro settimane), benché breve, avesse consentito di trarre conclusioni precise riguardo alla vita privata degli interessati, costituendo perciò una grave ingerenza nella stessa. Ha ritenuto inoltre che la normativa nazionale che garantiva il pieno rispetto delle condizioni stabilite dalla giurisprudenza interpretativa della direttiva 2002/58 in materia di accesso ai dati conservati non potesse, per sua natura, essere idonea a limitare e neppure a riparare la grave ingerenza risultante dalla conservazione generalizzata di tali dati. La CGUE ha sottolineato in proposito per quanto riguarda le garanzie previste dalla normativa nazionale oggetto dei procedimenti principali (volte a proteggere i dati conservati dai rischi di abuso e da qualsiasi accesso illecito) che ciascuna occorrenza di conservazione e accesso a tali dati costituiva un'ingerenza distinta nei diritti fondamentali garantiti dagli articoli 7 e 11 della Carta che richiedeva una giustificazione distinta ai sensi dell'articolo 52 § 1 della medesima.

88. In tale sentenza la CGUE ha anche considerato la giurisprudenza della Corte, citata da alcuni governi in relazione a cause analoghe; ha osservato che le sentenze *Big Brother Watch e altri c. Regno Unito* ([GC], nn. 58170/13 e altri 2, 25 maggio 2021) e *Centrum för rättvisa c. Svezia* ([GC], n. 35252/08, 25 maggio 2021) non potevano rimettere in discussione l'interpretazione dell'articolo 15 § 1 della direttiva 2002/58 concernente la conservazione generalizzata e indiscriminata dei dati relativi al traffico e all'ubicazione. Ha rilevato che tali sentenze riguardavano intercettazioni di massa di dati relative a comunicazioni internazionali e la Corte non si era pronunciata sulla conformità alla Convenzione di una conservazione generalizzata e indiscriminata di dati relativi al traffico e di dati relativi all'ubicazione nel territorio nazionale né tantomeno di un'intercettazione di ampia portata di tali dati ai fini della prevenzione, dell'accertamento e della ricerca di reati gravi. La CGUE ha poi osservato che l'articolo 52 § 3 della Carta mirava a garantire la necessaria coerenza tra i diritti contenuti in quest'ultima e i diritti corrispondenti garantiti dalla CEDU, senza pregiudicare l'autonomia del diritto dell'Unione e della CGUE, sicché occorreva tenere conto dei diritti corrispondenti della CEDU ai fini dell'interpretazione della Carta solo quale soglia di protezione minima.

IN DIRITTO

I. OSSERVAZIONI PRELIMINARI

89. La Corte osserva che, in risposta alle osservazioni del Governo, il ricorrente ha sollevato un nuovo rilievo concernente l'asserito preconcetto

della giudice V.L. derivante dalla sua conoscenza di certi elementi di prova che erano stati esclusi dal fascicolo penale. A giudizio della Corte il nuovo rilievo sollevato dal ricorrente non è un’elaborazione della doglianza originale proposta dinanzi alla Corte in data 21 aprile 2020 e comunicata al Governo. Menzionato soltanto per inciso, non contiene una base fattuale e giuridica sufficiente a qualificarlo come “doglianza” ai sensi della giurisprudenza della Corte (si veda *Radomilja e altri c. Croazia* [GC], nn. 37685/10 e 22768/12, § 126, 20 marzo 2018). La Corte, pertanto, non procederà al suo esame.

II. SULLA DEDOTTA VIOLAZIONE DELL’ARTICOLO 6 DELLA CONVENZIONE

90. Il ricorrente ha lamentato il rifiuto da parte del tribunale di primo grado di consentire l’esame di E.R. e M.S. in qualità di testimoni al processo. Ha lamentato anche che non si poteva ritenere imparziale la giudice del tribunale che lo aveva condannato, dato il suo ruolo nel procedimento a carico di E.R. e M.S. e il contenuto della sentenza da lei pronunciata nei loro confronti. Ha invocato l’articolo 6 §§ 1 e 3 lettera d) della Convenzione, che recita:

“1. Ogni persona ha diritto a che la sua causa sia esaminata equamente, (...) da un tribunale (...) il quale sia chiamato a pronunciarsi (...) sulla fondatezza di ogni accusa penale formulata nei suoi confronti.

(...)

3. In particolare, ogni accusato ha diritto di:

(...)

(d) esaminare o far esaminare i testimoni a carico e ottenere la convocazione e l’esame dei testimoni a discarico nelle stesse condizioni dei testimoni a carico;

(...)”

A. Sulla ricevibilità

91. La Corte osserva che tale parte del ricorso non è manifestamente infondata né incorre negli altri motivi di irricevibilità elencati dall’articolo 35 della Convenzione. Deve pertanto essere dichiarata ricevibile.

B. Sul merito

1. Gli argomenti delle parti

92. Il ricorrente ha sostenuto che l’esame di M.S. e E.R. sarebbe servito a corroborare la sua difesa, ovvero il suo tentativo di dimostrare che non aveva mai chiesto o ricevuto pagamenti da E.Č. e che il denaro che aveva ricevuto da M.S. gli era in realtà stato dato come rimborso di un prestito. Nessuno dei

due imputati, presunti intermediari del reato asseritamente commesso dal ricorrente, aveva dichiarato, prima delle rispettive ammissioni di colpevolezza, che il ricorrente aveva loro chiesto del denaro. Inoltre M.S. non aveva spiegato perché aveva dato EUR 8.000 al ricorrente. Tale punto, però, avrebbe potuto essere chiarito se al ricorrente fosse stata data la possibilità di interrogarlo. Inoltre, le comunicazioni registrate di nascosto ampiamente invocate nella sentenza riguardavano M.S. e E.R. Il tribunale distrettuale le aveva interpretate a danno del ricorrente che non aveva potuto chiarirne il contenuto esaminando M.S. e E.R.

93. Il ricorrente ha poi sostenuto che, dopo la confessione di M.S. e E.R. gli si sarebbe dovuta dare la possibilità di un confronto con loro. Ha osservato che (contrariamente a quanto affermato dai tribunali interni) la sentenza contro di lui aveva citato la dichiarazione di M.S. e vi aveva fatto riferimento all'atto del rigetto della sua difesa riguardante il rimborso del summenzionato prestito. In ordine alla tesi secondo la quale M.S. e E.R. non potevano essere esaminati in ragione della loro qualità di imputati, il ricorrente ha sostenuto che il tribunale interno avrebbe semplicemente potuto rinviare il procedimento per attendere che la sentenza nei loro confronti passasse in giudicato. Ha sottolineato che essa era divenuta definitiva il giorno seguente alla sua condanna. In ordine al rilievo del Governo, che aveva osservato che il ricorrente non aveva chiesto di essere autorizzato a interrogare i coimputati, il ricorrente ha sostenuto che in ogni caso egli non avrebbe potuto costringerli a rispondere alle domande dal momento che avevano optato per il silenzio ed erano protetti dal diritto a non autoincriminarsi. Ha sottolineato inoltre che quando M.S. aveva rilasciato la sua dichiarazione nel corso delle indagini né lui, né il suo rappresentante avevano avuto la possibilità di essere presenti.

94. Il ricorrente ha osservato anche che dal momento che la giudice V.L. aveva accettato l'ammissione di colpevolezza di E.R. e M.S. ella aveva perso l'apparenza di imparzialità. Per condannare E.R. e M.S. aveva dovuto valutare la causa nel merito, e il fatto che li avesse dichiarati colpevoli implicava che ella dovesse ritenere colpevole anche il ricorrente. Era questo il motivo per cui aveva successivamente rigettato tutte le richieste finalizzate all'acquisizione di prove e aveva proceduto a pronunciare la sentenza di colpevolezza nei confronti del ricorrente.

95. Il Governo ha osservato che gli atti di intermediazione della corruzione commessi da E.R. e M.S. dipendevano dal fatto che il ricorrente avesse preteso o accettato il compenso illecito in questione. Esso ritiene importante la circostanza che le loro ammissioni di colpevolezza siano state effettuate quasi alla fine del procedimento e che la sentenza nei confronti del ricorrente non vi abbia fatto riferimento.

96. In ordine al rigetto della richiesta di esame di E.R. e M.S. formulata dal ricorrente, il Governo ha sottolineato che E.R. non aveva voluto difendersi nel procedimento e che M.S. aveva voluto parlare in propria difesa soltanto quando era stato interrogato dal giudice istruttore. Il ricorrente aveva espresso

commenti in ordine alla dichiarazione di M.S. ma non aveva mai chiesto l'autorizzazione a porgli domande. Il Governo ha osservato inoltre che le sentenze impugnate avevano fatto riferimento alla dichiarazione di M.S. soltanto per corroborare le conclusioni fattuali formulate sulla base delle altre prove prodotte; rinviando alle conclusioni dei tribunali interni il Governo ha sostenuto che, date le circostanze del caso di specie, l'esame di M.S. e E.R. non era giustificato.

2. La valutazione della Corte

(a) Il rifiuto di consentire l'esame di E.R. e M.S.

(i) Osservazione preliminare

97. La Corte osserva che il ricorrente ha dedotto la violazione del suo diritto ai sensi dell'articolo 6 § 1 e 6 § 3 lettera d) perché il giudice del merito (la giudice V.L.) aveva rifiutato di consentire l'esame di E.R. e M.S. Osserva inoltre che l'articolo 6 § 3 lettera d) sancisce il diritto dell'imputato di esaminare o far esaminare i testimoni a carico e di convocare testimoni a discarico. Poiché i principi riguardanti l'esame dell'osservanza nel procedimento interno dell'articolo 6 § 3 lettera d) per alcuni aspetti sono distinti (si vedano *Al-Khawaja e Tahery c. Regno Unito* [GC], nn. 26766/05 e 22228/06, §§ 118-47, CEDU 2011, e *Schatschaschwili c. Germania* [GC], n. 9154/10, §§ 110-31, CEDU 2015, per quanto riguarda i testimoni dell'accusa; si veda altresì *Murtazaliyeva c. Russia* [GC], n. 36658/05, §§ 150-68, 18 dicembre 2018, per quanto riguarda i testimoni della difesa), la Corte ritiene necessario chiarire se la doglianza del ricorrente riguardi l'esame dei testimoni dell'accusa o il diritto di convocare testimoni per la difesa. A tale proposito la Corte osserva che essa sinora non ha specificato i criteri per distinguere le due categorie di testimoni nel contesto dell'articolo 6 § 3 lettera d).

98. Nel caso di specie il ricorrente nelle sue osservazioni dinanzi ai tribunali interni ha menzionato E.R. e M.S. talvolta come testimoni a suo carico (si veda il paragrafo 32 *supra*) e talvolta come testimoni della difesa (si veda il paragrafo 34 *supra*). Per determinare se la sua doglianza concerna in sostanza il diritto dell'imputato di esaminare o far esaminare i testimoni a carico o quello di convocare testimoni per la difesa, la Corte deve analizzare i motivi addotti per la richiesta di esame dei testimoni in questione del ricorrente. Osserva che M.S. ha reso una dichiarazione durante le indagini quando, a quanto risulta, né il ricorrente né il suo difensore erano presenti e quindi in grado di osservare e reagire. Tuttavia, non sembra che il ricorrente, chiamando M.S. in qualità di testimone, volesse soltanto verificare la dichiarazione piuttosto limitata rilasciata da quest'ultimo durante le indagini. Il ricorrente aveva richiesto l'esame di E.R. e M.S. per dimostrare che avevano agito per conto proprio e che egli (ovvero il ricorrente) non aveva mai ricevuto il pagamento iniziale e che aveva creduto che il denaro ricevuto

da M.S. fosse il rimborso di un prestito che gli aveva accordato. La Corte ritiene che gli argomenti addotti dal ricorrente dinanzi ai tribunali interni e nel procedimento dinanzi alla Corte (si vedano i paragrafi 29-32, 43, 46, 92 e 93, *supra*) indichino che la sua richiesta di esame di E.R. e M.S. era sostanzialmente volta a sostenere la sua difesa dalle imputazioni penali contestategli. Alla luce di quanto precede, e osservando che E.R. non aveva testimoniato al procedimento e che la sentenza a carico del ricorrente non citava le dichiarazioni rese da E.R. e M.S. nell'ambito delle loro ammissioni di colpevolezza, la Corte esaminerà la doglianza del ricorrente ai sensi dell'articolo 6 §§ 1 e 3 lettera d) sotto il profilo del diritto a convocare testimoni per la difesa.

(ii) *Principi generali*

99. La Corte ribadisce che, ai sensi dell'articolo 6 della Convenzione, l'ammissibilità delle prove è una materia che deve essere disciplinata principalmente dal diritto nazionale e che non compete alla Corte pronunciarsi sulla correttezza dell'ammissione di deposizioni di testimoni quali prove, le compete bensì accertare l'equità del procedimento nel suo complesso (comprese le modalità di assunzione delle prove) (si vedano, tra molti altri precedenti, *Van Mechelen e altri c. Paesi Bassi*, 23 aprile 1997, § 50, *Reports* 1997-III, e *Perna c. Italia* [GC], n. 48898/99, § 29, CEDU 2003-V). L'articolo 6 § 3 lettera d) della Convenzione non esige la convocazione e l'esame di ciascun testimone a discarico; semmai lo scopo essenziale di tale disposizione (indicato dalle parole “nelle stesse condizioni”) è quello di assicurare una piena “parità delle armi” relativamente alla questione in esame (si vedano *Engel e altri c. Paesi Bassi*, 8 giugno 1976, § 91, serie A n. 22; *Vidal c. Belgio*, 22 aprile 1992, § 33, serie A n. 235-B; e *Murtazaliyeva*, sopra citata, § 139).

100. Nella causa *Murtazaliyeva* (sopra citata, § 158) la Corte ha formulato il seguente triplice criterio per valutare l'osservanza del diritto a convocare testimoni per la difesa ai sensi dell'articolo 6 § 3 lettera d): (1) la richiesta di esame di un testimone è stata sufficientemente motivata ed era rilevante per l'oggetto dell'accusa?; (2) i tribunali interni hanno valutato la rilevanza di tale testimonianza e motivato a sufficienza la decisione di non consentire l'esame di un testimone al processo?; e (3) la decisione dei tribunali interni di non consentire l'esame di un testimone ha pregiudicato l'equità complessiva del procedimento?

101. In ordine al primo elemento, la Corte ha ritenuto che sia necessario esaminare la capacità della deposizione del testimone di influire sull'esito del processo o se ci si possa ragionevolmente attendere che essa rafforzi la posizione della difesa. La “sufficienza” delle motivazioni delle richieste di esame dei testimoni presentate dalla difesa dipende dalla valutazione delle circostanze del caso di specie, tra cui figurano le disposizioni del diritto interno applicabili, la fase e l'evoluzione del procedimento, le linee di

ragionamento e le strategie adottate dalle parti e la loro condotta procedurale (*ibid.*, §§ 160-61).

102. In ordine al secondo elemento del criterio, la Corte ha spiegato che generalmente la rilevanza di una testimonianza e la sufficienza dei motivi addotti dalla difesa nelle circostanze della causa determina la portata e a quale livello di dettaglio è svolta dai tribunali interni la valutazione della necessità di garantire la presenza e l'esame di un testimone. Pertanto quanto più solidi e importanti sono gli argomenti proposti dalla difesa tanto più attento deve essere l'esame e tanto più convincenti devono essere i motivi addotti dai tribunali interni qualora rifiutino la richiesta di esame di un testimone della difesa (*ibid.*, § 166).

103. In ordine alla valutazione dell'equità complessiva (il terzo elemento del criterio) la Corte ha sottolineato nella causa *Murtazaliyeva* che occorre esaminare il rispetto dei requisiti dell'equo processo in ciascuna causa, tenendo conto degli sviluppi del procedimento nel suo insieme e non sulla base della valutazione isolata di un particolare aspetto o di un particolare episodio. Benché le conclusioni derivanti dai primi due elementi del criterio siano generalmente fortemente indicative dell'equità o meno del procedimento, non si può escludere che in alcuni casi (dichiaratamente eccezionali) considerazioni di equità possano giustificare la conclusione opposta (*ibid.*, §§ 167-68).

(iii) *Applicazione dei principi al caso di specie*

104. La Corte osserva che il ricorrente e i due coimputati (E.R. e M.S.) sono stati processati insieme sino all'11 dicembre 2013 (data della diciannovesima udienza, si vedano i paragrafi 27 e 54 *supra*). A quel punto erano già state acquisite ampie prove, ma né il ricorrente né E.R. o M.S. si erano difesi attivamente. Quando, l'11 dicembre 2013, E.R. e M.S. si erano dichiarati colpevoli, la giudice V.L. aveva accettato le loro rispettive ammissioni di colpevolezza. Di conseguenza il ricorrente aveva chiesto, senza successo, l'esclusione della giudice V.L. dal procedimento a suo carico in ragione della sua asserita mancanza di imparzialità. Due giorni dopo, il 13 dicembre 2013, la giudice V.L. aveva separato il procedimento nei confronti di E.R. e M.S. e il 16 dicembre 2013 li aveva condannati per il reato continuato di favoreggiamento della corruzione del ricorrente. Nel corso delle udienze del procedimento (che ora riguardava soltanto il ricorrente) svoltesi il 13 e il 19 dicembre 2013 il ricorrente aveva rilasciato una dichiarazione difensiva e aveva inoltre chiesto l'esame di E.R. e M.S. in qualità di testimoni e il rinvio del procedimento fino a quando tale esame sarebbe divenuto possibile (si vedano i paragrafi 32 e 34 *supra*). La giudice V.L. aveva rigettato la richiesta spiegando che la sentenza nei confronti di E.R. e M.S. non era definitiva (il che significava che essi non potevano ancora essere esaminati in qualità di testimoni) e che erano state addotte prove sufficienti a consentirle di pronunciarsi sulle imputazioni a carico del ricorrente. Il 23 dicembre 2013

la giudice V.L. aveva dichiarato il ricorrente colpevole del reato continuato di corruzione in atti giudiziari. Due giorni più tardi la sentenza nei confronti di E.R. e M.S. era divenuta definitiva (si vedano i paragrafi 24-37 *supra*).

105. La Corte osserva che nella sua richiesta di esame di E.R. e M.S. presentata attraverso il suo rappresentante, il ricorrente aveva sostenuto, *inter alia*, che M.S. avrebbe potuto fornire informazioni in merito al prestito menzionato dal ricorrente nella sua dichiarazione difensiva; che E.R. avrebbe potuto testimoniare in merito ai debiti che E.Ć. aveva verso di lui e che egli avrebbe dimostrato che E.R. e M.S. non gli avevano detto di aver chiesto denaro a suo nome. Aveva sostenuto che non essendo più questi ultimi coimputati nello stesso procedimento potevano essere esaminati in qualità di testimoni (si vedano i paragrafi 29-32 *supra*). La Corte osserva inoltre che: la condanna del ricorrente era largamente fondata su prove relative a conversazioni tra M.S., E.R., E.Ć. e il ricorrente che i tribunali erano chiamati a interpretare nel contesto dato; la testimonianza verbalizzata di E.Ć. relativa agli eventi iniziali presentava incongruenze (si vedano i paragrafi 10, 21 e 41 *supra*); e M.S. e E.R., che asseritamente avevano svolto un ruolo cruciale nel favorire la commissione da parte del ricorrente del reato dedotto, non erano stati sentiti durante il processo. Data la loro iniziale qualità di imputati e la loro volontà di non difendersi (si veda il paragrafo 25 *supra*), la Corte non ritiene di particolare rilevanza il fatto che il ricorrente non avesse presentato una richiesta affinché fossero chiamati in qualità di testimoni prima della loro condanna (si veda il paragrafo 96 *supra*).

106. Alla luce delle suindicate considerazioni la Corte non è persuasa dell'insufficiente fondatezza della richiesta del ricorrente affinché M.S. e E.R. fossero chiamati in qualità di testimoni o della sua ininfluenza sull'oggetto delle accuse a suo carico. In altre parole, non ritiene che l'eventuale testimonianza di M.S. e E.R. non sarebbe stata in grado di influire sull'esito del processo o che non ci si sarebbe potuto ragionevolmente attendere che rafforzasse la posizione della difesa (si veda *Murtazaliyeva*, sopra citata, §§ 160-61).

107. In ordine al secondo elemento del criterio formulato nella causa *Murtazaliyeva* (si veda il paragrafo 102 *supra*), la Corte osserva che la giudice V.L. ha fornito alcuni motivi per il rigetto della richiesta di esame di E.R. e M.S. (si vedano i paragrafi 33-34 *supra*). In primo luogo, ha osservato che non aveva fondato la sua valutazione delle prove sull'ammissione di colpevolezza di M.S. e E.R. Tuttavia, come sopra indicato, il ricorrente aveva chiesto che, almeno nella sostanza, M.S. e E.R. fossero chiamati per conto della difesa. Il fatto che l'accusa non avesse fondato la sua tesi sulle ammissioni di colpevolezza di M.S. e E.R. non può essere ritenuto importante sotto questo profilo. Lo stesso vale per l'argomento che la condanna del ricorrente non era basata esclusivamente o in misura determinante sulla dichiarazione di M.S. (si veda il paragrafo 53 *supra*). Quanto alla circostanza che i tribunali interni avessero citato il fatto che il ricorrente aveva reso la sua

dichiarazione difensiva soltanto in una fase tardiva del procedimento (si vedano i paragrafi 33, 34, 48 e 53 *supra*), la Corte osserva che egli non aveva modificato la sua versione dei fatti, piuttosto l'aveva proposta soltanto dopo la confessione di M.S. e E.R. Non spetta alla Corte formulare congetture sul motivo di tale strategia difensiva, però, in ogni caso, si trattava di un suo diritto e nulla suggerisce che si possa considerare la sua condotta un tentativo di abusare dei suoi diritti procedurali.

108. In secondo luogo, in ordine alla tesi dei tribunali interni secondo la quale l'esame di M.S. e E.R. era impossibile perché la sentenza nei loro confronti non era passata in giudicato (in altre parole, in quel momento erano ancora coimputati, si vedano i paragrafi 33, 34, 48 e 53 *supra*), la Corte, date le circostanze della causa, non ritiene convincente tale ragionamento. Osserva che la giudice V.L. era ovviamente a conoscenza del termine di otto giorni per la dichiarazione dell'intenzione di impugnare da parte di M.S. e E.R. (si veda il paragrafo 36 *supra*). Da lei, in quanto massimo custode dell'equità del procedimento, ci si attendeva che misurasse attentamente le conseguenze delle sue decisioni procedurali sui diritti di difesa del ricorrente (si veda, *mutatis mutandis*, *Kikabidze c. Georgia*, n. 57642/12, § 59, 16 novembre 2021). Pur non potendo ovviamente sapere in quella fase se M.S. e E.R. si sarebbero avvalsi della possibilità di impugnazione, sembra che nulla le impedisse di rinviare l'udienza per attendere la scadenza di detto breve termine (otto giorni), in particolare dato che la sentenza nei confronti di M.S. e E.R. era basata sulle loro ammissioni di colpevolezza e dunque era ragionevolmente poco probabile che la impugnassero. La Corte ritiene pertanto che i tribunali interni non abbiano motivato a sufficienza il rifiuto di chiamare M.S. e E.R. a testimoniare.

109. Infine, in ordine all'equità complessiva del procedimento, la Corte osserva che all'apparenza la testimonianza di M.S. e E.R. sarebbe stata importante, dato che erano gli unici testimoni in grado di confermare o confutare la versione degli eventi fornita dal ricorrente nella sua dichiarazione difensiva (si vedano i paragrafi 29-32 *supra*). Alla luce degli sviluppi del procedimento era impossibile anticipare nella fase in questione in che modo M.S. e E.R., se fossero stati chiamati a testimoniare, avrebbero risposto alla versione dei fatti del ricorrente. Ugualmente non si può presumere che la produzione di tali testimonianze non avrebbe avuto alcuna incidenza sull'esito del processo. Il fatto che il ricorrente sia stato privato della possibilità di presentare in modo efficace prove testimoniali e di farle valere a propria difesa ha pertanto reso iniquo il processo.

110. Alla luce delle suesposte considerazioni la Corte conclude che il procedimento penale nei confronti del ricorrente non ha rispettato l'articolo 6 §§ 1 e 3 lettera d) della Convenzione. I tribunali interni che hanno esaminato i ricorsi proposti dal ricorrente non hanno riparato tale vizio.

111. Conseguentemente vi è stata violazione dell'articolo 6 §§ 1 e 3 lettera d) della Convenzione.

(b) Sull'asserita mancanza di imparzialità della giudice V.L.

112. La Corte, alla luce della summenzionata constatazione di violazione dell'articolo 6 §§ 1 e 3 lettera d) della Convenzione, ritiene che non sia necessario esaminare se vi sia stata anche violazione dell'articolo 6 § 1 a causa dell'asserita mancanza di imparzialità della giudice V.L. (si veda il paragrafo 90 *supra*).

III. SULLA DEDOTTA VIOLAZIONE DELL'ARTICOLO 8 DELLA CONVENZIONE

113. Il ricorrente ha lamentato che la conservazione dei dati relativi alle telecomunicazioni concernenti le sue attività di telecomunicazione il loro utilizzo nel procedimento a suo carico aveva violato l'articolo 8 della Convenzione, che recita:

“1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.

2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.”

A. Sulla ricevibilità

114. La Corte osserva che la presente doglianza non è manifestamente infondata né incorre negli altri motivi di irricevibilità elencati dall'articolo 35 della Convenzione. Deve pertanto essere dichiarata ricevibile.

B. Sul merito

1. Gli argomenti delle parti

115. Il ricorrente ha osservato che le pertinenti disposizioni della legge del 2004 come modificata e della legge del 2012 abrogate dalla Corte costituzionale erano identiche. Invocando la sentenza della CGUE (si vedano i paragrafi 74-76 *supra*) e la decisione della Corte costituzionale del 3 luglio 2014 (si vedano i paragrafi 66-68 *supra*), ha sostenuto che la memorizzazione dei dati in questione era contraria all'articolo 8 *ab initio* e che, di conseguenza, pure la loro acquisizione e utilizzo violavano la Costituzione e la Convenzione. A tale riguardo ha citato anche la discrepanza tra le conclusioni della Corte suprema nel procedimento penale da un lato, e quelle formulate nel procedimento disciplinare dall'altro (si veda il paragrafo 47 *supra*). Ha sostenuto inoltre che l'articolo 149.b della LPP (si veda il paragrafo 57 *supra*) avrebbe dovuto limitare l'accesso ai dati conservati soltanto ai reati gravi.

116. Secondo il ricorrente, inoltre, visto che i dati ottenuti nel suo caso erano stati viziati dall'incostituzionalità della legislazione in virtù della quale erano stati conservati non avrebbero dovuto essere utilizzati come prove nel suo processo. Ha aggiunto che non si doveva operare una distinzione tra i dati ottenuti prima e dopo la relativa decisione della Corte costituzionale (si vedano i paragrafi 66-68 *supra*). Tale distinzione costituiva una disparità di trattamento. La memorizzazione dei dati, che costituiva una violazione del suo diritto al rispetto della vita privata, non poteva essere validata *ex post* dai tribunali in specifici procedimenti affermando che la memorizzazione in questione era stata di fatto proporzionata. Il ricorrente ha anche sottolineato che l'articolo 149.b della LPP (si veda il paragrafo 57 *supra*) non aveva costituito il fondamento per la conservazione dei dati bensì per l'acquisizione dei dati conservati. In ordine al riferimento della Corte costituzionale alle "strutture commerciali" relativo alla memorizzazione dei dati (si veda il paragrafo 55 *supra*), il ricorrente ha sostenuto che tale rilievo si fondava su una semplice possibilità e non equivaleva a ritenere che la memorizzazione fosse stata in realtà legittima.

117. Il Governo, che nelle sue osservazioni ha soprattutto ribadito le conclusioni della Corte costituzionale (si vedano i paragrafi 66-68 *supra*), ha sostenuto che nel caso di specie i dati erano stati legittimamente acquisiti dal fornitore di servizi di telecomunicazione in virtù della pertinente normativa che all'epoca era valida. Ha sottolineato che le disposizioni della legge del 2004 come modificata, che erano alla base della memorizzazione dei dati del ricorrente, non erano state invalidate con effetto *ex tunc*. Benché la misura in questione avesse permesso di formulare deduzioni precise in ordine alle vite private degli interessati (ovvero all'intensità, al luogo, all'ora e alla durata delle comunicazioni tra E.R., M.S., E.Ć. e il ricorrente), si trattava di una misura necessaria, data la natura del presunto reato e del pubblico interesse coinvolto. I motivi per sospettare la commissione del reato di corruzione erano sufficientemente fondati. Il Governo ha sottolineato inoltre che la Corte costituzionale, che in seguito aveva invalidato le disposizioni di legge impugnate, non aveva ordinato la distruzione dei dati in questione (che a quel punto erano già stati acquisiti dai tribunali). Inoltre, un fondamento giuridico per la conservazione dei dati in questione era reperibile anche nell'articolo 104(2) della legge del 2004 come modificata che consentiva la conservazione dei dati per fini commerciali. Infine, secondo il Governo i dati relativi alle telecomunicazioni non erano stati memorizzati o destinati all'utilizzo in un procedimento disciplinare, pertanto le relative prove erano state giustamente escluse dal fascicolo di tale procedimento (si veda il paragrafo 47 *supra*).

2. La valutazione della Corte

(a) Principi e giurisprudenza pertinenti

118. La Corte ha già stabilito che i dati relativi all’abbonato, al traffico e all’ubicazione possono, da soli o congiuntamente, riguardare la “vita privata” degli interessati (si veda *Ekimdzhiev e altri c. Bulgaria*, n. 70078/12, § 372, 11 gennaio 2022). Ha inoltre costantemente ritenuto che la semplice conservazione di dati relativi alla vita privata di una persona costituisca un’ingerenza nel diritto di tale persona al rispetto della sua “vita privata” (*ibid.*; si vedano altresì *Breyer c. Germania*, n. 50001/12, § 81, 30 gennaio 2020, e *Centrum för rättvisa c. Svezia* [GC], n. 35252/08, § 244, 25 maggio 2021). Costituisce altresì un’ingerenza nel suo diritto al rispetto della corrispondenza (si vedano *Ekimdzhiev e altri*, sopra citata, § 373, e *Ben Faiza c. Francia*, n. 31446/12, §§ 66-67, 8 febbraio 2018). Il successivo utilizzo dei dati memorizzati non incide su tale conclusione (si vedano *Amann c. Svizzera* [GC], n. 27798/95, § 69, CEDU 2000-II, e *Trajkovski e Chipovski c. Macedonia del Nord*, nn. 53205/13 e 63320/13, § 51, 13 febbraio 2020). A ogni modo l’accesso da parte delle autorità ai dati conservati costituisce un’ulteriore ingerenza nel diritto al rispetto della vita privata e delle comunicazioni di cui all’articolo 8 della Convenzione (si veda *Ekimdzhiev e altri*, sopra citata, § 376; si vedano altresì, *mutatis mutandis*, *Centrum för rättvisa*, sopra citata, § 244, e *Big Brother Watch e altri c. Regno Unito* [GC], nn. 58170/13 e altri 2, § 330, 25 maggio 2021).

119. La Corte ribadisce che per via degli sviluppi tecnologici e sociali nel campo delle comunicazioni elettroniche, i dati di comunicazione oggi giorno posso rivelare una grande quantità di informazioni personali. Quando le autorità li acquisiscono in massa, tali dati possono essere utilizzati per tracciare un ritratto intimo della persona, *inter alia*, grazie alla mappatura delle sue attività sui social network, dei suoi spostamenti, delle sue abitudini di comunicazione nonché alla conoscenza delle persone con cui ha interagito (si vedano *Centrum för rättvisa*, § 256, e *Big Brother Watch e altri*, § 342, entrambe sopra citate). L’acquisizione di tali dati mediante intercettazioni di massa può pertanto essere altrettanto intrusiva dell’acquisizione in massa del contenuto delle comunicazioni, motivo per cui la loro intercettazione, conservazione e le ricerche su di essi effettuate dalle autorità devono essere analizzate in riferimento alle stesse garanzie applicabili al contenuto delle comunicazioni (si vedano *Centrum för rättvisa*, § 277, e *Big Brother Watch e altri*, § 363, entrambe sopra citate). Tale conclusione si applica anche alla conservazione generalizzata di dati di comunicazione da parte dei fornitori di servizi di comunicazione e all’accesso ad essi da parte delle autorità in singoli casi, che devono essere accompagnati, *mutatis mutandis*, dalle stesse garanzie inerenti alla sorveglianza segreta (si veda *Ekimdzhiev e altri*, sopra citata, § 395).

120. Qualsiasi ingerenza nei diritti ai sensi dell'articolo 8 può essere giustificata ai sensi dell'articolo 8 § 2 soltanto qualora sia prevista dalla legge, persegua uno o più fini legittimi indicati in tale paragrafo e sia necessaria in una società democratica per conseguire tali fini (si vedano *Roman Zakharov c. Russia* [GC], n. 47143/06, § 227, CEDU 2015, e *Kennedy c. Regno Unito*, n. 26839/05, § 130, 18 maggio 2010). Nelle cause in cui dinanzi alla Corte è contestata la legislazione che consente la sorveglianza segreta, la legittimità dell'ingerenza è strettamente collegata alla questione di sapere se sia stato rispettato il criterio della "necessità"; è pertanto opportuno che la Corte tratti congiuntamente il requisito della "previsione per legge" e della "necessità". In tal senso la "qualità della legge" implica non soltanto che il diritto interno debba essere accessibile e la sua applicazione prevedibile, ma anche che debba assicurare che le misure di sorveglianza segreta siano applicate soltanto qualora ciò sia "necessario in una società democratica", in particolare prevedendo tutele e garanzie adeguate ed effettive contro gli abusi (si vedano *Roman Zakharov*, § 236; *Kennedy*, § 155; e *Big Brother Watch e altri*, § 334, tutte sopra citate).

121. In linea generale, in ordine alla protezione dei dati personali, la Corte, nella causa *S. e Marper c. Regno Unito* [GC], nn. 30562/04 e 30566/04, § 103, CEDU 2008, ha ritenuto:

"La protezione di dati personali è di fondamentale importanza ai fini del godimento individuale del diritto al rispetto della vita privata e familiare garantito dall'articolo 8 della Convenzione. La legislazione interna deve prevedere garanzie idonee a impedire qualsiasi utilizzo di dati personali che non sia conforme alle garanzie sancite da tale disposizione (...) La necessità di tali garanzie risulta essere ancora maggiore allorché è in gioco la protezione di dati personali sottoposti a trattamenti automatizzati e in particolare quando tali dati sono utilizzati a fini di indagini di polizia. Il diritto interno dovrebbe assicurare in particolare che siffatti dati siano pertinenti e non eccessivi in relazione alle finalità per le quali essi sono conservati, e che siano conservati in una forma che consenta l'identificazione del titolare degli stessi per un periodo non eccedente quello che è strettamente necessario per le finalità per le quali essi sono memorizzati (si veda l'articolo 5 della Convenzione sulla protezione dei dati (...)) [nel paragrafo 47 *supra*]. Il diritto interno deve altresì prevedere garanzie adeguate in grado di assicurare che i dati personali conservati siano efficacemente protetti da utilizzazioni improprie ed abusive (si veda, in particolare, l'articolo 7 della Convenzione sulla protezione dei dati [nel paragrafo 47 *supra*]) (...)"

122. I principi che regolano la questione di sapere quando le misure di sorveglianza (compresa l'intercettazione delle comunicazioni) siano giustificabili ai sensi dell'articolo 8 § 2 della Convenzione sono dettagliatamente indicati nella causa *Roman Zakharov* (sopra citata, §§ 227-34, 236, 243, 247, 250, 257-58, 275, 278 e 287-88) e sono stati recentemente adattati al contesto delle intercettazioni di massa nelle cause *Centrum för rättvisa* (sopra citata, §§ 246-53 e 262-64) e *Big Brother Watch e altri* (sopra citata, §§ 332-39 e 348-50).

123. In ordine all'intercettazione di massa di dati relativi a comunicazioni internazionali, la Corte ha ritenuto che l'intensità dell'ingerenza nei diritti

protetti dall'articolo 8 aumenti man mano che il processo avanza (*Big Brother Watch e altri*, sopra citata, § 325). Ha osservato però che anche il semplice fatto di conservare dei dati relativi alla vita privata di un individuo costituisce un'ingerenza ai sensi dell'articolo 8 (*ibid.*, § 330). A tale proposito, La Corte ha ritenuto imperativo che, quando uno Stato mette in atto un regime di intercettazione di massa, il diritto interno contenga norme dettagliate che prevedano le circostanze nelle quali le autorità possono ricorrere a tali misure. Il quadro giuridico interno dovrebbe, in particolare, esprimere con sufficiente chiarezza i motivi per i quali può essere autorizzata un'intercettazione di massa. Inoltre, come stabilito dalla precedente giurisprudenza, il diritto interno deve definire il termine della durata dell'intercettazione, la procedura da seguire per l'esame, l'utilizzo e la conservazione dei dati raccolti, le precauzioni da adottare per la comunicazione dei dati ad altre parti e le circostanze nelle quali i dati intercettati possono o devono essere cancellati o distrutti (*ibid.*, § 348; si veda altresì *Centrum för rättvisa*, sopra citata, § 262). Nel medesimo contesto la Corte ha ritenuto che allo scopo di ridurre quanto più possibile il rischio di abuso delle intercettazioni di massa, il processo debba essere inquadrato da «garanzie end-to-end», il che significa che (i) a livello nazionale la necessità e la proporzionalità delle misure adottate dovrebbero essere valutate in ciascuna fase del processo, (ii) che le attività di intercettazione di massa dovrebbero essere soggette all'autorizzazione di un'autorità indipendente fin dall'inizio, fin dalla definizione dell'oggetto e della portata dell'operazione, e (iii) che le operazioni dovrebbero essere oggetto di una supervisione e di un controllo indipendente operato *a posteriori* (si vedano *Big Brother Watch e altri*, § 350, e *Centrum för rättvisa*, § 264, entrambe sopra citate).

124 In ordine alla questione di sapere se l'ingerenza fosse “necessaria in una società democratica” per perseguire un fine legittimo, le autorità nazionali godono di un certo margine di discrezionalità riguardo alla scelta dei mezzi per conseguire i fini legittimi di, *inter alia*, proteggere la sicurezza nazionale o prevenire e perseguire i reati. Tale margine è tuttavia soggetto alla vigilanza europea, che abbraccia sia la legislazione che le decisioni che la applicano e considera tutte le circostanze della causa, quali la natura, la portata e la durata delle eventuali misure, i motivi necessari per disporle, le autorità competenti ad autorizzarle, eseguirle e controllarle, e il tipo di rimedio previsto dal diritto nazionale (si vedano *Roman Zakharov*, § 232, e *Breyer*, § 79, entrambe sopra citate).

(b) La valutazione della Corte nel caso di specie

(i) Portata dell'esame

125. La Corte osserva che i dati relativi al traffico e all'ubicazione (in prosieguo anche “i dati relativi alle comunicazioni” o, qualora ci si riferisca specificamente alla telefonia, “i dati relativi alle telecomunicazioni”)

concernenti il ricorrente nel caso di specie erano stati acquisiti dagli organi di polizia in conformità a decreti del tribunale fondati su motivi che giustificavano il sospetto che il ricorrente (che all'epoca era un magistrato) fosse implicato in atti di corruzione, ovvero in un reato di grave natura. Osserva inoltre che, a parte il rilievo sulla portata dei decreti che autorizzavano l'accesso, che non era limitata ai reati gravi (si veda il paragrafo 115 *supra*), non era stata addotta alcuna ragione per mettere in discussione l'adeguatezza di tali decreti o il quadro giuridico nel quale erano stati emessi. Tuttavia nel caso di specie la questione che suscita preoccupazione in relazione all'articolo 8 riguarda il regime soggiacente alla collocazione dei dati relativi alle telecomunicazioni dai quali sono stati ottenuti quelli del ricorrente per le finalità del procedimento penale nei suoi confronti. Per accertare se l'ingerenza costituita da tale conservazione fosse "prevista dalla legge" e proporzionata, la Corte deve esaminare la legge slovena che disciplinava la conservazione dei dati in vigore all'epoca in questione.

126. La Corte osserva che i dati relativi alle telecomunicazioni del ricorrente, come quelli di ogni altro utente di servizi di telecomunicazione, all'epoca erano stati conservati ai sensi dell'articolo 107.a della legge del 2004 come modificata, che recepiva le pertinenti disposizioni della direttiva sulla conservazione dei dati (si veda il paragrafo 64 *supra*). Suddetta disposizione imponeva ai fornitori di servizi di comunicazione elettronica di conservare per un periodo di quattordici mesi, *inter alia*, i dati relativi alle comunicazioni inerenti alla telefonia fissa e mobile per una serie di scopi, ovvero per finalità di procedura penale e di salvaguardia della sicurezza nazionale, dell'ordine costituzionale, della sicurezza, degli interessi politici ed economici dello Stato e per la difesa nazionale. Occorre sottolineare che i dati del ricorrente non erano stati conservati allo scopo specifico di prevenire o indagare su reati gravi ma per le summenzionate finalità. L'ingerenza nei suoi diritti protetti dall'articolo 8, costituita dalla conservazione dei suoi dati, deve pertanto essere esaminata alla luce di tale più ampio contesto.

127. Ciò premesso, i dati in questione sono stati consultati e trattati nel procedimento penale nei confronti del ricorrente, il che ha provocato la sua doglianza. Nel corso del procedimento penale i tribunali interni, compresa la Corte costituzionale, hanno esaminato nel merito la questione di cui è ora investita la Corte.

(ii) *Sulla sussistenza di un'ingerenza*

128. Nel caso di specie è pacifico che la conservazione dei dati relativi alle telecomunicazioni del ricorrente e l'accesso ad essi e il loro trattamento da parte delle autorità abbia costituito un'ingerenza nei suoi diritti tutelati dall'articolo 8 della Convenzione. La Corte, avuto riguardo alla propria giurisprudenza (si veda il paragrafo 118 *supra*), non vede motivo di ritenere altrimenti. Essa ritiene inoltre che l'ingerenza concernente la conservazione

dei dati da parte dei fornitori di servizi di comunicazione era richiesta dalla legge ed era pertanto attribuibile allo Stato sloveno (si veda *Ekimdzhiev e altri*, sopra citata, § 375).

129. La Corte deve ora esaminare se l'ingerenza fosse giustificata ai sensi dell'articolo 8 § 2 della Convenzione, ovvero se fosse prevista dalla legge, perseguisse un fine legittimo e fosse "necessaria in una società democratica".

(iii) *Giustificazione dell'ingerenza*

(α) "Prevista dalla legge"

130. Le parti concordano sul fatto che all'epoca in questione la conservazione dei dati relativi alle telecomunicazioni aveva un fondamento giuridico sufficientemente chiaro costituito dalla legge del 2004 come modificata (si veda il paragrafo 64 *supra*), ed era pertanto prevedibile. L'accesso a tali dati era stato autorizzato dai decreti del tribunale distrettuale di Lubiana in virtù dell'articolo 149.b della LPP (si vedano i paragrafi 12-17 e 57 *supra*). In proposito occorre osservare che risulta che tali decreti indicassero un periodo eccedente quello autorizzato dalla legge. A ogni modo i fornitori di servizi in questione avevano memorizzato i dati soltanto per il periodo di quattordici mesi previsto dalla legge e avevano consegnato alle autorità soltanto tali dati (ovvero quelli relativi a un periodo non eccedente quattordici mesi) (si veda il paragrafo 17 *supra*). L'ingerenza in questione sotto questo profilo era quindi conforme alla normativa interna in vigore all'epoca dei fatti. Ciò detto, la Corte osserva che dopo l'acquisizione dei dati relativi alle telecomunicazioni nella causa del ricorrente, la Corte costituzionale, (si vedano i paragrafi 66-68 *supra*), sulla scorta della sentenza della CGUE nella causa *Digital Rights Ireland e altri* (si vedano i paragrafi 74-76 *supra*), aveva dichiarato che il regime di conservazione dei dati ai sensi della legge del 2012 (che sotto questo profilo era sostanzialmente identico a quello previsto dalla legge del 2004 come modificata) violava i diritti relativi alla vita privata degli utenti dei servizi di comunicazione elettronica. La Corte terrà conto di tale pronuncia nell'esaminare la "necessità" dell'ingerenza che, in questo tipo di cause, è strettamente collegata alla "legittimità" (si veda il paragrafo 120 *supra*).

(β) Fine legittimo

131. È incontestato che il regime di conservazione dei dati in esame perseguisse i fini legittimi indicati nel secondo paragrafo dell'articolo 8. La Corte reputa che si possa ritenere che il regime di conservazione in questione perseguisse i fini della sicurezza nazionale, della pubblica sicurezza o del benessere economico del paese, della difesa dell'ordine e della prevenzione dei reati, o della protezione dei diritti e delle libertà altrui. Si può ritenere che l'accesso ai dati relativi alle telecomunicazioni del ricorrente e il loro

trattamento perseguissero il fine legittimo della prevenzione dei reati e della protezione dei diritti e delle libertà altrui.

(γ) “Necessaria in una società democratica”

– *Livello di ingerenza*

132. Il caso di specie non concerne l’intercettazione diretta di dati da parte delle autorità, sebbene riguardi i rischi di tale intercettazione. In virtù delle impugnate disposizioni di legge, i fornitori di servizi avevano l’obbligo giuridico di raccogliere e memorizzare i dati relativi alle telecomunicazioni (in misura eccedente quella necessaria a fini di fatturazione o altri fini contrattuali) per tenerli a disposizione delle autorità. La maggior parte di tali dati non veniva mai consultata. Sotto questo profilo il caso di specie è paragonabile alla causa *Breyer* (sopra citata), nella quale l’ingerenza lamentata consisteva nell’obbligo giuridico in capo ai fornitori di servizi di raccogliere e memorizzare le generalità degli utenti di schede SIM mobili prepagate (unitamente ai relativi numeri telefonici) al fine di mettere, su richiesta, tali dati a disposizione delle autorità (*ibid.*, §§ 76-77).

133. Tuttavia, a differenza della causa *Breyer*, che concerneva un’ingerenza di natura limitata (*ibid.*, § 95), il caso di specie concerne i dati relativi alle telecomunicazioni (si veda l’articolo 107.b della legge del 2004 come modificata, citato al paragrafo 64 *supra*) che, qualora siano associati a un abbonato o a un utente, possono rivelare aspetti intimi della sua vita, grazie alla mappatura delle sue attività sui social network, dei suoi spostamenti, delle sue abitudini di comunicazione nonché alla conoscenza delle persone con cui ha interagito (si vedano *mutatis mutandis*, *Ekimdzhiev e altri*, § 394; *Centrum för rättvisa*, § 256; e *Big Brother Watch e altri*, § 342, tutte sopra citate). A giudizio della Corte, la sorveglianza sistemica comportata dalla conservazione obbligatoria dei dati relativi alle telecomunicazioni rappresenta un impedimento al godimento dei diritti relativi alla vita privata di tutti gli utenti dei servizi di telecomunicazione. L’esistenza di vaste raccolte di dati relativi alle telecomunicazioni e la conservazione perdurante di tali dati può comprensibilmente generare un senso di fragilità e vulnerabilità e può compromettere la capacità degli interessati di godere della vita privata e della riservatezza della corrispondenza, di sviluppare relazioni interpersonali e di esercitare altri diritti fondamentali. A tale riguardo la Corte rinvia anche alle osservazioni formulate dalla CGUE nella causa *Digital Rights Ireland e altri* laddove afferma che i dati relativi alle comunicazioni presi nel loro complesso, possono permettere “di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati” e che la loro conservazione e trattamento costituisce pertanto “un’ingerenza di vasta portata e di particolare gravità” nei loro diritti fondamentali (si veda il paragrafo 76 *supra*). La gravità dell’ingerenza è stata riconosciuta anche

dal Governo convenuto (si veda il paragrafo 117 *supra*) e dalla Corte costituzionale slovena (si vedano i paragrafi 55 e 66-68 *supra*).

134. Alla luce delle suesposte considerazioni la Corte ritiene che l'ingerenza costituita dalla conservazione dei dati in esame fosse di grave natura. Deve ora determinare se i mezzi previsti dalla normativa impugnata per il conseguimento dei fini legittimi (si veda il paragrafo 131 *supra*) abbiano rispettato i requisiti del principio dello Stato di diritto e siano rimasti sotto ogni profilo entro i limiti di ciò che è necessario in una società democratica.

– *Ampiezza del margine di discrezionalità*

135. Sebbene tale punto non sia stato dimostrato da nessun dato empirico, la Corte non dubita che il tracciamento del traffico relativo alle telecomunicazioni, consentito dall'obbligo di conservazione fissato dalla normativa impugnata, potesse avere considerevole importanza per l'effettiva applicazione della legge e per l'adozione di efficaci misure di pubblica sicurezza. Ribadisce che il contrasto alla criminalità (in particolare alla criminalità organizzata e al terrorismo, che costituisce una delle sfide cui devono far fronte le odierne società europee), la tutela della pubblica sicurezza e dei cittadini costituiscono "pressanti esigenze sociali" (si veda *Breyer*, sopra citata, § 88). Riconosce altresì che i moderni mezzi di telecomunicazione e i mutamenti nelle modalità di comunicazione richiedono un adattamento degli strumenti investigativi a disposizione delle forze dell'ordine e delle agenzie per la sicurezza nazionale (si veda *S. e Marper*, sopra citata, § 105).

136. Ciò premesso, affinché un'ingerenza sia conforme al secondo paragrafo dell'articolo 8 non è sufficiente che essa sia idonea o efficace a promuovere il fine in questione; deve essere anche proporzionata ovvero conseguire un giusto equilibrio tra i pubblici interessi concorrenti e i diritti sanciti dalla Convenzione (si vedano *Handyside c. Regno Unito*, 7 dicembre 1976, § 48, serie A n. 24; *Breyer*, sopra citata, § 91; e *Szabó e Vissy c. Ungheria*, n. 37138/14, § 55, 12 gennaio 2016). È innegabile che nel contesto della tutela della sicurezza nazionale o della prevenzione e del perseguimento dei reati, le autorità nazionali godano di un certo margine di discrezionalità nella scelta dei mezzi per conseguire un fine legittimo (si veda il paragrafo 124 *supra*). Esso tuttavia rimane soggetto al controllo della Corte e la sua ampiezza dipende da una serie di fattori determinati dal caso di specie. Il margine tende a essere più ristretto qualora il diritto in gioco sia cruciale per l'effettivo godimento di diritti di carattere intimo o fondamentale o qualora l'ingerenza sia di vasta portata (si veda *S. e Marper*, sopra citata, § 102; si confrontino altresì *Dubská e Krejzová c. Repubblica ceca* [GC], nn. 28859/11 e 28473/12, § 178, 15 novembre 2016; *Dudgeon c. Regno Unito*, 22 ottobre 1981, § 52, serie A n. 45; e *National Union of Rail, Maritime and Transport Workers c. Regno Unito*, n. 31045/10, §§ 86-87, CEDU 2014). Pertanto,

tenuto conto della natura e della gravità dell'ingerenza in gioco, la Corte deve svolgere un esame conseguentemente più rigoroso quando valuta la questione del giusto equilibrio (nonché delle necessarie garanzie) nel caso di specie (si veda, per contro, *Breyer*, sopra citata, §§ 94-96 e 103).

– *La valutazione del “giusto equilibrio”*

137. La Corte osserva che benché le disposizioni di legge che disciplinano il trattamento dei dati relativi alle comunicazioni possano essere diverse da quelle che regolano la sorveglianza dei contenuti delle comunicazioni, esse devono essere analizzate con riferimento alle stesse garanzie applicabili ai contenuti (si veda, *mutatis mutandis*, *Big Brother Watch e altri*, sopra citata, § 416). La conservazione generalizzata dei dati relativi alle comunicazioni da parte dei fornitori di servizi di comunicazione e la loro consultazione da parte delle autorità in singoli casi devono pertanto essere accompagnati, *mutatis mutandis*, dalle stesse garanzie previste per la sorveglianza segreta (*Ekimdzhiev e altri*, sopra citata [cl41284](#), § 395). Nella sua giurisprudenza sulle misure di sorveglianza nell'ambito delle indagini penali, la Corte ha sviluppato le seguenti garanzie minime che devono essere previste dalla legge per evitare abusi di potere: natura dei reati che possono dare luogo a un decreto di intercettazione; definizione delle categorie di persone le cui comunicazioni possono essere intercettate; limite alla durata delle intercettazioni; procedura da seguire per l'esame, l'utilizzo e la conservazione dei dati raccolti; precauzioni da adottare per la comunicazione dei dati a terzi; e circostanze in cui i dati intercettati possono o debbono essere cancellati o distrutti (si vedano *Weber e Saravia c. Germania* (dec.), n. 54934/00, CEDU 2006-XI, e *Liberty e altri c. Regno Unito*, n. 58243/00, 1° luglio 2008). Nella causa *Roman Zakharov* (sopra citata, § 231) – che concerneva anche altri fini di interesse pubblico come la tutela della sicurezza nazionale, la Corte ha formulato le garanzie applicabili in modo analogo, dando ulteriore rilievo ai meccanismi di notifica e ai rimedi previsti dal diritto nazionale. Ha fondato la sua valutazione della conformità all'articolo 8 dei provvedimenti di intercettazione in questione sui seguenti criteri: accessibilità del diritto interno pertinente, campo di applicazione e durata delle misure di sorveglianza segreta, procedure da seguire per conservare, accedere, esaminare, utilizzare, comunicare e distruggere i dati intercettati, procedure di autorizzazione, modalità di vigilanza sull'attuazione delle misure di sorveglianza segreta, gli eventuali meccanismi di notificazione e i ricorsi previsti dal diritto nazionale (*ibid.*, § 238). Nell'ambito delle intercettazioni di massa di comunicazioni internazionali, nelle cause *Big Brother Watch e altri* (sopra citata, § 361) e *Centrum för rättvisa* (sopra citata, § 275), la Corte ha ulteriormente messo a punto suddetti criteri, in particolare il requisito che il diritto interno definisca chiaramente i motivi per i quali l'intercettazione di massa può essere autorizzata, le circostanze nelle quali le comunicazioni di

un individuo possono essere intercettate e la procedura di concessione di un'autorizzazione.

138. In ordine al caso di specie la Corte osserva che la legge del 2004 come modificata imponeva, per diversi fini di pubblico interesse, la conservazione per un periodo di quattordici mesi di tutti i dati relativi alle comunicazioni generati o trattati nel corso della fornitura dei relativi servizi pubblici di comunicazione (si veda il paragrafo 64 *supra*). La legge non sembrava lasciare alcuna decisione in materia alla discrezionalità di qualsivoglia organo statale o non statale ed era priva di ambiguità riguardo alla sua applicazione. Ciascun individuo o ente che utilizzava i servizi dei fornitori di telecomunicazioni della Slovenia poteva prevedere la conservazione dei propri dati relativi alle telecomunicazioni quale parte di un'estesa raccolta di dati. Tuttavia non si poteva ritenere che la chiarezza della legge, che fissava la regola della conservazione generalizzata e indiscriminata dei dati relativi alle telecomunicazioni, costituisse una garanzia sufficiente della sua conformità ai principi dello Stato di diritto e di proporzionalità.

139. La Corte osserva che nella causa *Ekimdzhiiev e altri* (sopra citata), che concerneva un regime analogo disciplinante la conservazione dei dati relativi alle comunicazioni, essa si è concentrata sulle garanzie relative all'accesso ai dati conservati e alla conservazione dei dati consultati; non si è pronunciata sulla conformità del regime di conservazione in quanto tale ai requisiti dell'articolo 8 (*ibid.*, §§ 394-421). Tuttavia nel caso di specie il ricorrente ha specificamente lamentato la conservazione dei dati relativi alle telecomunicazioni e il loro successivo utilizzo asseritamente avvenuti in violazione dell'articolo 8 (si vedano i paragrafi 125 e 126 *supra*). La Corte in proposito osserva che la legge del 2004 come modificata stabiliva una serie di fini che imponevano la conservazione dei dati relativi alle telecomunicazioni ma non conteneva disposizioni che limitassero la portata e l'applicazione della misura a quanto necessario per il conseguimento di tali fini, né è stata dimostrata l'esistenza di altri atti legislativi contenenti siffatte disposizioni. Dalla summenzionata giurisprudenza (si vedano i paragrafi 119-123 e 137 *supra*) discende l'obbligo che il diritto interno definisca, come parte dei requisiti minimi, in maniera adeguata alla particolare forma di sorveglianza, la portata dell'applicazione della misura in questione e preveda procedure idonee a disporla e/o controllarla al fine di mantenerla nei limiti di ciò che è necessario. Tenuto conto della natura dell'ingerenza in questione (si vedano i paragrafi 132-134 *supra*), anche la misura che comportava la conservazione dei dati relativi alle telecomunicazioni avrebbe dovuto soddisfare tali requisiti minimi. L'assenza di disposizioni o meccanismi per assicurare che la misura fosse effettivamente limitata a quanto era "necessario in una società democratica" per gli specifici fini elencati nella legge del 2004 come modificata ha reso tale regime inconciliabile con gli obblighi dello Stato ai sensi dell'articolo 8. Tale conclusione non può essere inficiata dalla

semplice limitazione del periodo di conservazione a quattordici mesi, che è un periodo di tempo considerevole.

140. La Corte osserva inoltre che la CGUE è pervenuta a una conclusione analoga nella sentenza *Digital Rights Ireland e altri*, che ha esaminato il regime di conservazione nella sua interezza, ovvero in relazione sia alla conservazione dei dati relativi alle telecomunicazioni che di alcuni dati relativi a internet. La CGUE ha ritenuto che il regime di conservazione obbligatoria generalizzata e indifferenziata dei dati relativi alle comunicazioni al fine della lotta contro i reati gravi non rispettasse il requisito di proporzionalità (si vedano i paragrafi 74-76 *supra*; si vedano altresì le conclusioni della CGUE nelle successive sentenze che hanno chiarito e sviluppato ulteriormente i requisiti e che sono riassunte ai paragrafi 77, 78, 82, 84 e 87 *supra*). La Corte costituzionale, con decisione del 3 luglio 2014 (si vedano i paragrafi 66-68 *supra*), ha parimenti dichiarato invalide le disposizioni che disciplinavano la conservazione dei dati relativi alle comunicazioni della legge del 2012 (che erano essenzialmente uguali a quelle della legge del 2004 come modificata) e ha fatto riferimento alla summenzionata sentenza della CGUE. Nella sua giurisprudenza successiva la CGUE ha chiarito che anche nel contesto della salvaguardia della sicurezza nazionale, nel quale era possibile - a certe condizioni - ordinare la conservazione dei dati relativi alle comunicazioni quale misura generalizzata e indiscriminata, tale conservazione non poteva avere carattere sistemico e, una volta disposta, doveva essere soggetta a controllo indipendente (si veda il paragrafo 78 *supra*).

141. In ordine alla specifica situazione del ricorrente, la Corte osserva che è pacifico che i dati relativi alle telecomunicazioni del ricorrente all'epoca dei fatti furono conservati in maniera sistemica, generalizzata e indiscriminata in virtù della legge del 2004 come modificata. Tali dati, conservati per un periodo di quattordici mesi, furono acquisiti dalle autorità ai fini di un'indagine penale intrapresa nei confronti del ricorrente. Furono poi trattati dando origine ai rapporti analitici che furono depositati nel fascicolo penale dello stesso. Nel rigettare le doglianze relative alla vita privata del ricorrente, i tribunali interni hanno menzionato il fatto che (i) l'accesso ai dati in questione era avvenuto prima della dichiarazione di invalidità del pertinente regime, e (ii) che i decreti del tribunale che autorizzavano l'accesso ai dati erano fondati sul sospetto che fosse stato commesso un grave reato ed erano giustificati dalla proporzionalità della misura (si vedano i paragrafi 45, 51 e 55 *supra*). La Corte costituzionale aveva anche espresso l'opinione che i dati relativi alle telecomunicazioni citati nella sentenza di condanna del ricorrente si riferissero al breve periodo rispetto al quale essi potevano essere ottenuti dalle "strutture commerciali" (si veda il paragrafo 55 *supra*).

142. Rispetto a tali considerazioni la Corte reputa che non si possa ritenere che il fatto che il regime di conservazione sia stato dichiarato invalido dalla CGUE e dalla Corte costituzionale dopo l'accesso ai dati in questione

implichi che all'epoca dei fatti esso fosse conforme all'articolo 8. Ciò che conta è stabilire se quando avveniva la conservazione dei suoi dati relativi alle telecomunicazioni, il ricorrente godesse della tutela giuridica cui aveva diritto ai sensi della Convenzione. Alla luce delle conclusioni e delle considerazioni esposte nei paragrafi 137-140 *supra* la Corte ritiene che non sia stato così.

143. La Corte osserva inoltre che benché il ricorrente abbia chiaramente sostenuto che i dati relativi alle telecomunicazioni riguardanti le sue telecomunicazioni erano stati conservati in violazione dei suoi diritti relativi alla vita privata, i tribunali interni avevano limitato il loro esame quasi esclusivamente ai motivi per i quali i decreti giudiziari avevano autorizzato l'accesso ai dati conservati, sebbene essi (come osservato dalla Corte costituzionale) non fossero stati contestati dal ricorrente (si veda il paragrafo 55 *supra*). La Corte al riguardo vuole sottolineare che sebbene l'accesso ai suoi dati fosse accompagnato da alcune garanzie (per esempio dal controllo giudiziario), esse, pur facendo parte dei criteri da soddisfare, (si veda *Ekimdzhiev e altri*, sopra citata, §§ 360-421), non erano di per sé sufficienti a rendere il regime di conservazione conforme all'articolo 8. A titolo comparativo la Corte osserva che la CGUE in maniera analoga nella causa *SpaceNet e Telekom Deutschland* ha ritenuto che una normativa nazionale che garantiva il pieno rispetto delle condizioni stabilite dalla sua giurisprudenza interpretativa della direttiva sulla conservazione dei dati relativa all'accesso ai dati conservati non potesse, per sua stessa natura, essere idonea a limitare o anche a riparare una grave ingerenza derivante dalla conservazione generalizzata di tali dati, in quanto la conservazione e l'accesso a tali dati erano due ingerenze distinte che richiedevano giustificazioni distinte (si veda il paragrafo 87 *supra*).

144. Il ricorrente ha sostenuto inoltre che a causa dell'ingiustificata conservazione dei suoi dati, la loro acquisizione e utilizzo nel procedimento interno avevano violato l'articolo 8 (si vedano i paragrafi 115 e 116 *supra*). A tale proposito la Corte ritiene che quando si riscontra che la conservazione dei dati relativi alle telecomunicazioni viola l'articolo 8 perché non rispetta il requisito della "qualità della legge" e/o il principio di proporzionalità, l'accesso a tali dati, e il loro trattamento e conservazione successivi da parte delle autorità non possano, per il medesimo motivo, essere conformi all'articolo 8. A tale riguardo rinvia ancora una volta all'opinione espressa dalla CGUE. Nella causa *An Garda Síochána e altri* tale corte ha ritenuto che i dati relativi alle comunicazioni non potessero essere oggetto di conservazione generalizzata e indifferenziata ai fini della lotta alla criminalità grave e che, pertanto, l'accesso a tali dati non potesse essere giustificato a questi stessi fini (si veda il paragrafo 84 *supra*). La Corte nella causa del ricorrente non vede motivo per ritenere altrimenti.

145. La Corte osserva che nel caso di specie sussiste violazione, indipendentemente dal fatto che i dati conservati violando i diritti del

ricorrente ai sensi dell'articolo 8 fossero stati citati o meno dai tribunali interni per dichiarare la colpevolezza di quest'ultimo (si vedano i principi menzionati nel paragrafo 118 *supra* e nella causa *Huvig c. Francia*, 24 aprile 1990, § 35, serie A n. 176-B, nella quale le impugnate intercettazioni telefoniche in questione non erano servite da fondamento dell'azione penale). In proposito la Corte presume che la valutazione delle misure impugunate effettuata dai tribunali interni, anche dalla Corte costituzionale (si veda il paragrafo 55 *supra*), fosse strettamente collegata alla questione dell'ammissibilità delle prove raccolte in detto modo (si confronti *Dragojević c. Croazia*, n. 68955/11, §§ 99 e 100, 15 gennaio 2015), il che non è sorprendente perché essa è stata effettuata nell'ambito di un procedimento penale a carico del ricorrente ed era pertanto limitata alle finalità di tale procedimento (si veda il paragrafo 127 *supra*). Tuttavia ai fini dell'articolo 8 non ha alcuna particolare rilevanza il fatto che per condannare il ricorrente nel caso di specie i tribunali interni abbiano citato una parte limitata dei dati relativi alle telecomunicazioni in questione, che riguardavano un periodo di circa un mese e che avrebbero potuto essere conservati per finalità contrattuali (si veda il paragrafo 55 *supra*). La doglianza del ricorrente concerneva tutto l'insieme dei suoi dati relativi a un periodo di quattordici mesi, che erano stati acquisiti dagli organi di polizia e poi trattati, conservati ed esaminati per le finalità del procedimento penale in questione. È pacifico che tale quantità di dati non avrebbe potuto essere conservata per scopi contrattuali ma che era invece stata conservata nel quadro di un regime di conservazione generalizzata e indiscriminata che la Corte ha ritenuto *supra* contrario all'articolo 8 della Convenzione.

146. Infine, tenendo presente che le conclusioni relative alla doglianza del ricorrente ai sensi dell'articolo 8 non concernono l'ammissibilità delle prove raccolte a carico dello stesso, che è una questione che spetta ai tribunali interni valutare in conformità alla normativa interna applicabile, la Corte ribadisce che l'ammissione e l'utilizzo in un procedimento giudiziario di prove raccolte in violazione dell'articolo 8 non conduce necessariamente alla constatazione di violazione dell'articolo 6 (si veda *Bykov c. Russia* [GC], n. 4378/02, §§ 89-91, 10 marzo 2009, con ulteriori riferimenti).

– *Conclusione*

147. Alla luce delle suesposte considerazioni la Corte ritiene che le impugnate disposizioni della legge del 2004 come modificata che costituivano il fondamento della conservazione dei dati relativi alle telecomunicazioni del ricorrente non soddisfacevano il requisito della “qualità della legge” e non fossero idonee a limitare la “ingerenza” nei diritti del medesimo ai sensi dell'articolo 8 a quanto “necessario in una società democratica”. Pertanto, la conservazione, l'accesso e il trattamento di tali dati relativi alle telecomunicazioni hanno violato l'articolo 8 della Convenzione.

IV. SULL'APPLICAZIONE DELL'ARTICOLO 41 DELLA
CONVENZIONE

148. L'articolo 41 della Convenzione recita:

“Se la Corte dichiara che vi è stata violazione della Convenzione o dei suoi Protocolli e se il diritto interno dell'Alta Parte contraente non permette se non in modo imperfetto di rimuovere le conseguenze di tale violazione, la Corte accorda, se del caso, un'equa soddisfazione alla parte lesa.”

A. Danno

149. Il ricorrente ha chiesto 15.000 euro (EUR) per il danno non patrimoniale relativo alla violazione dell'articolo 6 della Convenzione ed EUR 5.000 per quello relativo alla violazione dell'articolo 8 della Convenzione, in totale EUR 20.000. Ha chiesto inoltre circa EUR 655.000 per il danno patrimoniale conseguente alla perdita del lavoro e quindi di reddito, alla multa impostagli e alla somma corrispondente al vantaggio economico ottenuto dal reato commesso (si veda il paragrafo 42 *supra*).

150. Il Governo ha ritenuto la richiesta di danno non patrimoniale eccessiva. Si è altresì opposto alla richiesta di danno patrimoniale sostenendo che la richiesta relativa alla perdita di reddito era infondata. Ha osservato che qualora il ricorrente fosse risultato vittorioso nel procedimento dinanzi alla Corte, egli avrebbe potuto chiedere la riapertura del procedimento penale. Secondo il Governo, pertanto, si sarebbe dovuto considerare la constatazione di violazione equa soddisfazione sufficiente.

151. La Corte non può formulare congetture circa quale sarebbe stato l'esito del processo nel caso in cui esso fosse stato conforme alla Convenzione, e osserva che, come confermato dal Governo, il ricorrente può chiedere la riapertura del procedimento dinanzi ai tribunali interni. Rigetta pertanto la sua richiesta di danno patrimoniale. D'altro canto riconosce che gli eventi che hanno provocato le violazioni riscontrate nel caso di specie hanno causato al ricorrente un danno non patrimoniale che non può essere riparato dalla semplice constatazione di violazione. La Corte, deliberando in via equitativa, accorda al ricorrente la somma di EUR 5.000 per il danno non patrimoniale, oltre l'importo eventualmente dovuto a titolo di imposta.

B. Spese

152. Il ricorrente ha chiesto anche EUR 6.928 (comprehensive di IVA) per le spese sostenute dinanzi alla Corte e EUR 14.960 per quelle sostenute nel corso dei procedimenti dinanzi ai tribunali interni.

153. Il Governo ha sostenuto che la richiesta di spese relativa ai procedimenti interni non era affatto documentata e che la richiesta relativa al procedimento dinanzi alla Corte era eccessiva.

154. Secondo la giurisprudenza della Corte, un ricorrente ha diritto al rimborso delle spese sostenute solo nella misura in cui ne siano accertate la realtà e la necessità, e il loro importo sia ragionevole. Nel caso di specie, tenuto conto della documentazione in suo possesso e dei suddetti criteri la Corte osserva che il ricorrente non ha documentato la sua richiesta relativa ai procedimenti dinanzi ai tribunali interni. Per quanto riguarda il procedimento dinanzi alla Corte, essa ritiene ragionevole accordare la somma di EUR 5.000 che copre tutte le voci di spesa, oltre l'importo eventualmente dovuto dal ricorrente a titolo di imposta.

PER QUESTI MOTIVI, LA CORTE, ALL'UNANIMITÀ,

1. *Dichiara* ricevibile il ricorso;
2. *Ritiene* che vi sia stata violazione dell'articolo 6 §§ 1 e 3 lettera d) della Convenzione per quanto riguarda il diritto del ricorrente di convocare testimoni a discarico;
3. *Ritiene* che non sia necessario esaminare il merito della doglianza ai sensi dell'articolo 6 § 1 della Convenzione riguardante l'imparzialità del giudice del merito;
4. *Ritiene* che vi sia stata violazione dell'articolo 8 della Convenzione;
5. *Ritiene*
 - (a) che lo Stato convenuto debba versare al ricorrente, entro tre mesi a decorrere dalla data in cui la sentenza sarà divenuta definitiva conformemente all'articolo 44 § 2 della Convenzione, le seguenti somme al tasso applicabile alla data del versamento:
 - (i) EUR 5.000 (cinquemila euro), oltre l'importo eventualmente dovuto a titolo di imposta, per il danno non patrimoniale;
 - (ii) EUR 5.000 (cinquemila euro), oltre l'importo eventualmente dovuto dal ricorrente a titolo di imposta, per le spese;
 - (b) che a decorrere da detto termine e fino al versamento tali importi dovranno essere maggiorati di un interesse semplice equivalente a quello delle operazioni di rifinanziamento marginale della Banca centrale europea applicabile durante tale periodo, maggiorato di tre punti percentuali;
6. *Rigetta* la domanda di equa soddisfazione del ricorrente per il resto.

SENTENZA ŠKOBERNE c. SLOVENIA

Fatta in inglese e notificata per iscritto il 15 febbraio 2024, in applicazione dell'articolo 77 §§ 2 e 3 del Regolamento della Corte.

Liv Tigerstedt
Cancelliere aggiunto

Alena Poláčková
Presidente