SENTENZA DELLA CORTE (Seconda Sezione)

19 ottobre 2016 ([\*](http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=IT" \l "Footnote*))

«Rinvio pregiudiziale – Trattamento dei dati personali – Direttiva 95/46/CE – Articolo 2, lettera a) – Articolo 7, lettera f) – Nozione di “dati personali” – Indirizzi di protocollo Internet – Conservazione da parte di un fornitore di servizi di media online – Normativa nazionale che non consente di prendere in considerazione l’interesse legittimo perseguito dal responsabile del trattamento»

Nella causa C‑582/14,

avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell’articolo 267 TFUE, dal Bundesgerichtshof (Corte di giustizia federale, Germania), con decisione del 28 ottobre 2014, pervenuta in cancelleria il 17 dicembre 2014, nel procedimento

**Patrick Breyer**

contro

**Bundesrepublik Deutschland,**

LA CORTE (Seconda Sezione),

sentite le conclusioni dell’avvocato generale, presentate all’udienza del 12 maggio 2016,

ha pronunciato la seguente

**Sentenza**

1        La domanda di pronuncia pregiudiziale verte sull’interpretazione dell’articolo 2, lettera a), e dell’articolo 7, lettera f), della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU 1995, L 281, pag. 31).

2        Tale domanda è stata presentata nell’ambito di una controversia tra il sig. Patrick Breyer e la Bundesrepublik Deutschland (Repubblica federale di Germania) in merito alla registrazione e alla conservazione, da parte di quest’ultima, dell’indirizzo di protocollo Internet (in prosieguo: l’«indirizzo IP») del sig. Breyer in occasione della consultazione fatta dal medesimo di vari siti Internet dei servizi federali tedeschi.

**Contesto normativo**

*Diritto dell’Unione*

3        Il considerando 26 della direttiva 95/46 è così formulato:

«considerando che i principi della tutela si devono applicare ad ogni informazione concernente una persona identificata o identificabile; che, per determinare se una persona è identificabile, è opportuno prendere in considerazione l’insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona; che i principi della tutela non si applicano a dati resi anonimi in modo tale che la persona interessata non è più identificabile; che i codici di condotta ai sensi dell’articolo 27 possono costituire uno strumento utile di orientamento sui mezzi grazie ai quali [i] dati possano essere resi anonimi e registrati in modo da rendere impossibile l’identificazione della persona interessata».

4        A termini dell’articolo 1 di detta direttiva:

«1.      Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali.

2.      Gli Stati membri non possono restringere o vietare la libera circolazione dei dati personali tra Stati membri, per motivi connessi alla tutela garantita a norma del paragrafo 1».

5        L’articolo 2 della medesima direttiva è del seguente tenore:

«Ai fini della presente direttiva si intende per:

a)      “dati personali”: qualsiasi informazione concernente una persona fisica identificata o identificabile (“persona interessata”); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero d’identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale;

b)      “trattamento di dati personali” (“trattamento”): qualsiasi operazione o insieme di operazioni compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l’organizzazione, la conservazione, l’elaborazione o la modifica, l’estrazione, la consultazione, l’impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, nonché il congelamento, la cancellazione o la distruzione;

(…)

d)      “responsabile del trattamento”: la persona fisica o giuridica, l’autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario;

(…)

f)      “terzi”: la persona fisica o giuridica, l’autorità pubblica, il servizio o qualsiasi altro organismo che non sia la persona interessata, il responsabile del trattamento, l’incaricato del trattamento e le persone autorizzate all’elaborazione dei dati sotto la loro autorità diretta;

(…)».

6        L’articolo 3 della direttiva 95/46, intitolato «Campo d’applicazione», stabilisce quanto segue:

«1.      Le disposizioni della presente direttiva si applicano al trattamento di dati personali interamente o parzialmente automatizzato nonché al trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi.

2.      Le disposizioni della presente direttiva non si applicano ai trattamenti di dati personali[:]

–        effettuati per l’esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del trattato sull’Unione europea e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale;

(…)».

7        L’articolo 5 della suddetta direttiva così dispone:

«Gli Stati membri precisano, nei limiti delle disposizioni del presente capo, le condizioni alle quali i trattamenti di dati personali sono leciti».

8        L’articolo 7 della stessa direttiva è formulato nel modo seguente:

«Gli Stati membri dispongono che il trattamento di dati personali può essere effettuato soltanto quando:

a)      la persona interessata ha manifestato il proprio consenso in maniera inequivocabile, oppure

b)      è necessario all’esecuzione del contratto concluso con la persona interessata o all’esecuzione di misure precontrattuali prese su richiesta di tale persona, oppure

c)      è necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento, oppure

d)      è necessario per la salvaguardia dell’interesse vitale della persona interessata, oppure

e)      è necessario per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati, oppure

f)      è necessario per il perseguimento dell’interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l’interesse o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell’articolo 1, paragrafo 1».

9        L’articolo 13, paragrafo 1, della direttiva 95/46 così dispone:

«Gli Stati membri possono adottare disposizioni legislative intese a limitare la portata degli obblighi e dei diritti previsti dalle disposizioni dell’articolo 6, paragrafo 1, dell’articolo 10, dell’articolo 11, paragrafo 1, e degli articoli 12 e 21, qualora tale restrizione costituisca una misura necessaria alla salvaguardia:

(…)

d)      della prevenzione, della ricerca, dell’accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate;

(…)».

*Diritto tedesco*

10      L’articolo 12 del Telemediengesetz (legge sui media online), del 26 febbraio 2007 (BGBl. 2007 I, pag. 179; in prosieguo: il «TMG»), così dispone:

«1)      Il fornitore di servizi può raccogliere e impiegare dati personali ai fini della messa a disposizione di media online solo nella misura in cui lo permetta la presente legge o un’altra norma, riguardante espressamente i media online, oppure se l’utente vi abbia prestato consenso.

2)      Il fornitore di servizi può impiegare ad altri fini i dati personali raccolti per la messa a disposizione di media online solo nella misura in cui lo permetta la presente legge o un’altra norma, riguardante espressamente i media online, oppure l’utente vi abbia prestato consenso.

3)      Ove non sia diversamente stabilito, le norme vigenti per la tutela dei dati personali trovano applicazione anche nel caso in cui i dati non costituiscano oggetto di trattamento automatizzato».

11      L’articolo 15 del TMG prevede quanto segue:

«1)      Il fornitore di servizi può raccogliere e impiegare i dati personali di un utente solo nella misura in cui ciò sia necessario per rendere possibile la fruizione di media online e per fatturarla (dati di utenza). Costituiscono dati di utenza, in particolare:

1.      gli elementi per l’identificazione dell’utente,

2.      le informazioni su inizio e termine, nonché sulla durata di ciascuna fruizione e

3.      le indicazioni sui media online fruiti dall’utente.

2)      Il fornitore di servizi può aggregare i dati di utenza di un utente attinenti alla fruizione di diversi media online, laddove ciò sia necessario a fini di fatturazione verso l’utente.

(…)

4)      Il fornitore di servizi può impiegare i dati di utenza oltre il termine della fruizione, ove essi siano necessari a fini di fatturazione verso l’utente (dati di fatturazione). Il fornitore di servizi può bloccare i dati ai fini dell’osservanza dei periodi di conservazione definiti per legge, statuto o contratto (…)».

12      Conformemente all’articolo 3, paragrafo 1, del Bundesdatenschutzgesetz (legge federale sulla protezione dei dati), del 20 dicembre 1990 (BGBl. 1990 I, pag. 2954) «[i] dati personali sono dati particolari su condizioni personali o materiali di una persona fisica identificata o identificabile (interessato) (…)».

**Procedimento principale e questioni pregiudiziali**

13      Il sig. Breyer ha consultato vari siti Internet dei servizi federali tedeschi. Su tali siti, accessibili al pubblico, i suddetti servizi forniscono informazioni aggiornate.

14      Al fine di contrastare attacchi e consentire il perseguimento penale dei «pirati informatici», nella maggior parte di detti siti tutti gli accessi sono registrati nei file di registro. In essi sono memorizzati, al termine della sessione di consultazione di tali siti, il nome del sito o del file consultato, le parole inserite nei campi di ricerca, la data e l’ora della consultazione, il volume dei dati trasferiti, il messaggio relativo all’esito della consultazione e l’indirizzo IP del computer a partire dal quale è stato effettuato l’accesso.

15      Gli indirizzi IP sono sequenze numeriche assegnate a computer collegati a Internet al fine di consentire la comunicazione tra i medesimi attraverso tale rete. In caso di consultazione di un sito Internet, l’indirizzo IP del computer che effettua l’accesso è trasmesso al server che ospita il sito consultato. Tale comunicazione è necessaria per inviare i dati richiesti al corretto destinatario.

16      Peraltro, dalla decisione di rinvio e dagli atti a disposizione della Corte emerge che i fornitori di accesso a Internet assegnano ai computer degli utenti di tale rete un indirizzo IP che può essere o «statico» o «dinamico», ossia un indirizzo IP che cambia a ogni nuova connessione a Internet. A differenza degli indirizzi IP statici, gli indirizzi IP dinamici non consentirebbero di associare, attraverso file accessibili al pubblico, un dato computer al collegamento fisico alla rete utilizzato dal fornitore di accesso a Internet.

17      Il sig. Breyer ha proposto un ricorso dinanzi ai giudici amministrativi tedeschi, chiedendo che alla Repubblica federale di Germania sia inibito di conservare o far conservare da terzi, al termine delle sessioni di consultazione dei siti accessibili al pubblico di media online dei servizi federali tedeschi, l’indirizzo IP del nodo ospite del sig. Breyer, qualora tale conservazione non sia necessaria, in caso di guasto, al ripristino della diffusione di detti media.

18      A seguito del rigetto in primo grado del ricorso del sig. Breyer, quest’ultimo ha proposto appello avverso la decisione di rigetto.

19      Il giudice di appello ha parzialmente riformato tale decisione. Esso ha condannato la Repubblica federale di Germania ad astenersi dal conservare o dal far conservare da terzi, al termine di ogni consultazione, l’indirizzo IP del nodo ospite del sig. Breyer, trasmesso all’atto della consultazione, da parte del medesimo, dei siti accessibili al pubblico di media online dei servizi federali tedeschi, qualora tale indirizzo sia conservato unitamente alla data della sessione di consultazione alla quale si riferisce e qualora il sig. Breyer abbia rivelato la propria identità durante tale sessione, anche sotto forma di un indirizzo elettronico che menzioni la sua identità, laddove tale conservazione non sia necessaria, in caso di guasto, al ripristino della diffusione di media online.

20      Secondo detto giudice di appello, un indirizzo IP dinamico, associato alla data della sessione di consultazione alla quale esso si riferisce, costituisce, nel caso in cui l’utente del sito Internet considerato abbia rivelato la propria identità durante tale sessione, un dato personale, poiché l’operatore di detto sito può identificare tale utente incrociando il suo nome con l’indirizzo IP del suo computer.

21      Il suddetto giudice di appello ha ritenuto che, tuttavia, il ricorso del sig. Breyer non meritasse accoglimento in altre ipotesi. Infatti, nel caso in cui il sig. Breyer non indichi la propria identità durante una sessione di consultazione, solamente il fornitore di accesso a Internet potrebbe ricollegare l’indirizzo IP a un abbonato identificato. Per contro, tra le mani della Repubblica federale di Germania, nella sua qualità di fornitore di servizi di media online, l’indirizzo IP non sarebbe un dato personale, neppure se associato alla data della sessione di consultazione alla quale esso si riferisce, dato che l’utente dei siti Internet considerati non sarebbe identificabile da parte di tale Stato membro.

22      Il sig. Breyer e la Repubblica federale di Germania hanno ciascuno proposto un ricorso per «Revision» (cassazione) dinanzi al Bundesgerichtshof (Corte federale di giustizia, Germania) avverso la decisione del giudice di appello. Il sig. Breyer chiede l’accoglimento integrale della sua domanda inibitoria. La Repubblica federale di Germania chiede il rigetto di tale domanda.

23      Il giudice del rinvio precisa che gli indirizzi IP dinamici del computer del sig. Breyer, conservati dalla Repubblica federale di Germania quando agisce come fornitore di media online, costituiscono, quanto meno nel contesto degli altri dati conservati nei file di registro, dati particolari su situazioni materiali del sig. Breyer, poiché forniscono indicazioni relative alla consultazione, da parte del medesimo, di determinati siti o di determinati file su Internet in determinate date.

24      Tuttavia, i dati così conservati non consentirebbero di determinare direttamente l’identità del sig. Breyer. Infatti, gli operatori dei siti Internet di cui al procedimento principale potrebbero identificare il sig. Breyer solamente se il fornitore di accesso a Internet del medesimo trasmettesse loro informazioni sull’identità di detto utente. La qualificazione di tali dati come «personali» dipenderebbe, di conseguenza, dalla possibilità o meno di identificare il sig. Breyer.

25      Il Bundesgerichtshof (Corte federale di giustizia) richiama la controversia dottrinale relativa alla scelta di un criterio «oggettivo» oppure di un criterio «relativo» al fine di stabilire se una persona sia identificabile. Applicando un criterio «oggettivo», dati come gli indirizzi IP discussi nel procedimento principale potrebbero essere qualificati, al termine delle sessioni di consultazione dei siti Internet considerati, come dati personali anche qualora solamente un terzo sia in grado di determinare l’identità della persona interessata, terzo che, nel caso di specie, è il fornitore di accesso a Internet del sig. Breyer che ha conservato dati aggiuntivi i quali consentono l’identificazione del medesimo attraverso i suddetti indirizzi IP. Secondo un criterio «relativo», dati siffatti potrebbero essere qualificati come dati personali nei confronti di un organismo, quale il fornitore di accesso a Internet del sig. Breyer, poiché consentono la precisa identificazione dell’utente (v., in tal senso, sentenza del 24 novembre 2011, Scarlet Extended, C‑70/10, EU:C:2011:771, punto 51), ma come privi di tale qualificazione nei confronti di un altro organismo, quale l’operatore dei siti Internet consultati dal sig. Breyer, dato che detto operatore non disporrebbe, nel caso in cui il sig. Breyer non abbia rivelato la propria identità nel corso delle sessioni di consultazione di detti siti, delle informazioni necessarie per identificarlo senza un eccessivo dispendio di risorse.

26      Nell’ipotesi in cui gli indirizzi IP dinamici del computer del sig. Breyer dovessero essere considerati, in associazione con la data della sessione alla quale si riferiscono, dati personali, il giudice del rinvio chiede se la conservazione di tali indirizzi IP al termine di detta sessione sia autorizzata ai sensi dell’articolo 7, lettera f), della medesima direttiva.

27      A tale riguardo, il Bundesgerichtshof (Corte federale di giustizia) precisa, da un lato, che i fornitori di servizi di media online possono, ai sensi dell’articolo 15, paragrafo 1, del TMG, raccogliere e impiegare dati personali di un utente solo nella misura in cui ciò sia necessario per consentire e fatturare la fruizione di detti media. Dall’altro, il giudice del rinvio indica che, secondo la Repubblica federale di Germania, la conservazione di tali dati è necessaria per garantire la sicurezza e la continuità del funzionamento dei siti dei servizi di media online che essa rende accessibili al pubblico, consentendo, in particolare, di riconoscere gli attacchi informatici detti «denial of service» («negazione di servizio»), volti a paralizzare il funzionamento di tali siti inondando in modo mirato e coordinato determinati server Internet di un gran numero di richieste, e di lottare contro simili attacchi.

28      Secondo il giudice del rinvio, se e nella misura in cui sia necessario che il fornitore di servizi di media online prenda misure per lottare contro simili attacchi, dette misure potrebbero essere considerate necessarie per «rendere possibile la fruizione di media online» ai sensi dell’articolo 15 del TMG. In dottrina viene però sostenuta prevalentemente la tesi secondo cui, da un lato, la raccolta e l’impiego dei dati personali di un utente di un sito Internet sono consentiti solo per rendere possibile una fruizione concreta di tale sito e, dall’altro, questi dati devono essere cancellati al termine della sessione di consultazione ove non necessari a fini di fatturazione. Orbene, una simile lettura restrittiva dell’articolo 15, paragrafo 1, del TMG osterebbe a che la conservazione degli indirizzi IP sia autorizzata per garantire, in maniera generale, la sicurezza e la continuità del funzionamento dei servizi online.

29      Il giudice del rinvio si chiede se quest’ultima interpretazione, che è quella suggerita dal giudice di appello, sia conforme all’articolo 7, lettera f), della direttiva 95/46, in particolare alla luce dei criteri enunciati dalla Corte ai punti 29 e seguenti della sentenza del 24 novembre 2011, ASNEF e FECEMD (C‑468/10 e C‑469/10, EU:C:2011:777).

30      In tale contesto, il Bundesgerichtshof (Corte federale di giustizia) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1)      Se l’articolo 2, lettera a), della direttiva 95/46 debba essere interpretato nel senso che un indirizzo IP memorizzato da un fornitore di servizi [di media online] in relazione ad un accesso al suo sito Internet costituisce per quest’ultimo un dato personale qualora sia un terzo (nel caso di specie: un fornitore di accesso) a disporre delle informazioni aggiuntive necessarie ai fini dell’identificazione della persona interessata.

2)      Se l’articolo 7, lettera f), [di tale direttiva] osti ad una disposizione di diritto nazionale in forza della quale il fornitore di servizi [di media online] può raccogliere e impiegare i dati personali di un utente senza il suo consenso solo nella misura in cui ciò sia necessario per consentire e fatturare l’effettiva fruizione del medium online da parte del rispettivo utente e secondo la quale il fine di assicurare il funzionamento in generale di detto medium non può giustificare l’impiego dei dati oltre il termine della rispettiva fruizione».

**Sulle questioni pregiudiziali**

*Sulla prima questione*

31      Con la sua prima questione, il giudice del rinvio chiede, in sostanza, se l’articolo 2, lettera a), della direttiva 95/46 debba essere interpretato nel senso che un indirizzo IP dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di tale fornitore, un dato personale ai sensi di detta disposizione qualora solamente un terzo, segnatamente il fornitore di accesso a Internet della suddetta persona, disponga delle informazioni necessarie a identificarla.

32      Ai sensi della summenzionata disposizione, per «dati personali» si intende «qualsiasi informazione concernente una persona fisica identificata o identificabile (“persona interessata”)». In base a tale disposizione, si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale.

33      In limine, si deve rilevare che, al punto 51 della sentenza del 24 novembre 2011, Scarlet Extended (C‑70/10, EU:C:2011:771), che verteva in particolare sull’interpretazione della medesima direttiva, la Corte ha dichiarato, in sostanza, che gli indirizzi IP degli utenti di Internet costituivano dati personali protetti, poiché consentono di identificare in modo preciso tali utenti.

34      Tuttavia, tale affermazione della Corte era relativa all’ipotesi in cui la raccolta e l’identificazione degli indirizzi IP degli utenti di Internet siano effettuati dai fornitori di accesso a Internet.

35      Orbene, nel caso in esame, la prima questione verte sull’ipotesi in cui sia il fornitore di servizi di media online, ossia la Repubblica federale di Germania, a registrare gli indirizzi IP degli utenti di un sito Internet che detto fornitore di servizi rende accessibile al pubblico, senza disporre delle informazioni aggiuntive necessarie per identificare tali utenti.

36      Inoltre, è pacifico che gli indirizzi IP ai quali il giudice del rinvio fa riferimento sono indirizzi IP «dinamici», ossia quelli, provvisori, assegnati ad ogni connessione a Internet e sostituiti in caso di successive connessioni, e non indirizzi IP «statici», che sono invariabili e consentono l’identificazione permanente del dispositivo connesso alla rete.

37      La prima questione posta dal giudice del rinvio si fonda quindi sulla premessa secondo cui, da un lato, dati consistenti in un indirizzo IP dinamico nonché nella data e nell’ora della sessione di consultazione di un sito Internet a partire da tale indirizzo IP, registrati da un fornitore di servizi di media online, non offrono, di per sé, a questo fornitore la possibilità di identificare l’utente che ha consultato detto sito Internet nel corso di tale sessione e, dall’altro, il fornitore di accesso a Internet dispone, quanto a lui, di informazioni aggiuntive che, se combinate con il suddetto indirizzo IP, consentirebbero di identificare l’utente in parola.

38      A tale riguardo, occorre anzitutto rilevare come sia pacifico che un indirizzo IP dinamico non costituisce un’informazione riferita a una «persona fisica identificata», dal momento che un indirizzo siffatto non rivela direttamente l’identità della persona fisica proprietaria del computer a partire dal quale avviene la consultazione di un sito Internet, né quella di un’altra persona che potrebbe utilizzare detto computer.

39      Inoltre, per determinare se un indirizzo IP dinamico costituisca, nell’ipotesi illustrata al punto 37 della presente sentenza, un dato personale ai sensi dell’articolo 2, lettera a), della direttiva 95/46 nei confronti di un fornitore di servizi di media online, occorre verificare se un indirizzo IP siffatto, registrato da un tale fornitore, possa essere qualificato come informazione riferita a una «persona fisica identificabile», qualora le informazioni aggiuntive necessarie per identificare l’utente di un sito Internet che detto fornitore di servizi rende accessibile al pubblico siano detenute dal fornitore di accesso a Internet dell’utente medesimo.

40      A tale riguardo, dalla formulazione dell’articolo 2, lettera a), della direttiva 95/46 risulta che si considera identificabile una persona che può essere identificata non solo direttamente, ma anche indirettamente.

41      L’uso da parte del legislatore dell’Unione del termine «indirettamente» indica tendenzialmente che, per qualificare un’informazione come dato personale, non è necessario che tale informazione consenta di per sé sola di identificare la persona interessata.

42      Inoltre, il considerando 26 della direttiva 95/46 enuncia che, per determinare se una persona sia identificabile, è opportuno prendere in considerazione l’insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona.

43      Nella misura in cui detto considerando fa riferimento ai mezzi che possono essere ragionevolmente utilizzati tanto dal responsabile del trattamento quanto da «altri», la sua formulazione suggerisce che, perché un dato possa essere qualificato come «dato personale» ai sensi dell’articolo 2, lettera a), di tale direttiva non si richiede che tutte le informazioni che consentono di identificare la persona interessata debbano essere in possesso di una sola persona.

44      Il fatto che le informazioni aggiuntive necessarie per identificare l’utente di un sito Internet siano detenute non dal fornitore di servizi di media online, ma dal fornitore di accesso a Internet di tale utente non pare quindi idoneo a escludere che gli indirizzi IP dinamici registrati dal fornitore di servizi di media online costituiscano, per quest’ultimo, dati personali ai sensi dell’articolo 2, lettera a), della direttiva 95/46.

45      Occorre tuttavia determinare se la possibilità di combinare un indirizzo IP dinamico con le suddette informazioni aggiuntive detenute da detto fornitore di accesso a Internet costituisca un mezzo che può essere ragionevolmente utilizzato per identificare la persona interessata.

46      Come in sostanza rilevato dall’avvocato generale al paragrafo 68 delle sue conclusioni, così non sarebbe se l’identificazione della persona interessata fosse vietata dalla legge o praticamente irrealizzabile, per esempio a causa del fatto che implicherebbe uno dispendio di tempo, di costo e di manodopera, facendo così apparire in realtà insignificante il rischio di identificazione.

47      Orbene, anche se il giudice del rinvio precisa, nella propria decisione di rinvio, che il diritto nazionale tedesco non consente al fornitore di accesso a Internet di trasmettere direttamente al fornitore di servizi di media online le informazioni aggiuntive necessarie all’identificazione della persona interessata, sembra tuttavia, ferme restando le verifiche che detto giudice dovrà compiere al riguardo, che esistano strumenti giuridici che consentono al fornitore di servizi di media online di rivolgersi, in particolare in caso di attacchi cibernetici, all’autorità competente affinché quest’ultima assuma le iniziative necessarie per ottenere tali informazioni dal fornitore di accesso a Internet e per avviare procedimenti penali.

48      Sembra quindi che il fornitore di servizi di media online disponga di mezzi che possono essere ragionevolmente utilizzati per identificare, con l’aiuto di altri soggetti, ossia l’autorità competente e il fornitore di accesso a Internet, la persona interessata sulla base degli indirizzi IP conservati.

49      Alla luce dell’insieme delle suesposte considerazioni, occorre rispondere alla prima questione che l’articolo 2, lettera a), della direttiva 95/46 dev’essere interpretato nel senso che un indirizzo IP dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di tale fornitore, un dato personale ai sensi di detta disposizione, qualora detto fornitore disponga di mezzi giuridici che gli consentano di far identificare la persona interessata grazie alle informazioni aggiuntive di cui il fornitore di accesso a Internet di detta persona dispone.

*Sulla seconda questione*

50      Con la sua seconda questione, il giudice del rinvio chiede, in sostanza, se l’articolo 7, lettera f), della direttiva 95/46 debba essere interpretato nel senso che osta a una normativa di uno Stato membro ai sensi della quale un fornitore di servizi di media online può raccogliere e impiegare dati personali di un utente di tali servizi, in mancanza del suo consenso, solo nella misura in cui detta raccolta e detto impiego siano necessari per consentire e fatturare l’effettiva fruizione dei suddetti servizi da parte dell’utente in questione, senza che l’obiettivo di assicurare il funzionamento generale dei medesimi servizi possa giustificare l’impiego di tali dati dopo una sessione di consultazione degli stessi.

51      Prima di rispondere a tale questione, occorre determinare se il trattamento dei dati personali di cui al procedimento principale, ossia gli indirizzi IP dinamici degli utenti di determinati siti Internet di servizi federali tedeschi, non sia escluso dal campo di applicazione della direttiva 95/46 in forza dell’articolo 3, paragrafo 2, primo trattino, della medesima, ai sensi del quale la suddetta direttiva non si applica al trattamento di dati personali aventi ad oggetto, tra l’altro, le attività dello Stato in materia di diritto penale.

52      A tale riguardo, occorre ricordare che le attività menzionate a titolo esemplificativo dalla suddetta disposizione sono, in tutti i casi, attività proprie degli Stati o delle autorità statali, estranee ai settori di attività dei privati (v. sentenze del 6 novembre 2003, Lindqvist, C‑101/01, EU:C:2003:596, punto 43, e del 16 dicembre 2008, Satakunnan Markkinapörssi e Satamedia, C‑73/07, EU:C:2008:727, punto 41).

53      Orbene, nella causa principale, ferme restando le verifiche che il giudice del rinvio dovrà compiere al riguardo, pare che i servizi federali tedeschi, che forniscono servizi di media online e che sono responsabili del trattamento degli indirizzi IP dinamici, agiscano, nonostante il loro status di pubbliche autorità, in qualità di soggetti privati e al di fuori dell’ambito delle attività dello Stato in materia di diritto penale.

54      Occorre pertanto determinare se una normativa di uno Stato membro, come quella di cui al procedimento principale, sia compatibile con l’articolo 7, lettera f), della direttiva 95/46.

55      A tal fine, occorre ricordare che la normativa nazionale discussa nel procedimento principale, come interpretata nel senso restrittivo prospettato dal giudice del rinvio, autorizza la raccolta e l’impiego dei dati personali di un utente di tali servizi, in mancanza del suo consenso, solamente nella misura in cui ciò sia necessario per consentire e fatturare l’effettiva fruizione del medium online da parte dell’utente in questione, senza che l’obiettivo di garantire il funzionamento generale del medium online possa giustificare l’impiego dei suddetti dati dopo una sessione di consultazione di tale medium.

56      Ai sensi dell’articolo 7, lettera f), della direttiva sulla tutela dei dati personali, il trattamento di dati personali è legittimo se «è necessario per il perseguimento dell’interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l’interesse o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell’articolo 1, paragrafo 1» di tale direttiva.

57      È importante ricordare che la Corte ha dichiarato che l’articolo 7 della suddetta direttiva prevede un elenco esaustivo e tassativo dei casi in cui il trattamento dei dati personali può essere considerato lecito, e che gli Stati membri non possono né aggiungere nuovi principi relativi alla legittimazione del trattamento dei dati personali del suddetto articolo né prevedere requisiti supplementari che vengano a modificare la portata di uno dei sei principi previsti da detto articolo (v., in tal senso, sentenza del 24 novembre 2011, ASNEF e FECEMD, C‑468/10 e C‑469/10, EU:C:2011:777, punti 30 e 32).

58      Anche se, certamente, l’articolo 5 della direttiva 95/46 autorizza gli Stati membri a precisare, nei limiti delle disposizioni del capo II di tale direttiva e, quindi, dell’articolo 7 della stessa, le condizioni alle quali i trattamenti dei dati personali sono leciti, il margine discrezionale di cui, in forza di detto articolo 5, dispongono gli Stati membri può essere utilizzato soltanto in conformità all’obiettivo perseguito dalla direttiva suddetta, consistente nel mantenere l’equilibrio tra la libera circolazione dei dati personali e la tutela della vita privata. Gli Stati membri non possono introdurre, sulla base dell’articolo 5 della stessa direttiva, principi relativi alla legittimazione del trattamento dei dati personali diversi da quelli enunciati all’articolo 7 della medesima, né modificare con requisiti supplementari la portata dei sei principi previsti da detto articolo 7 (v., in tal senso, sentenza del 24 novembre 2011, ASNEF e FECEMD, C‑468/10 e C‑469/10, EU:C:2011:777, punti 33, 34 e 36).

59      Nella fattispecie, risulta che l’articolo 15 del TMG, se interpretato nella maniera rigida menzionata al punto 55 della presente sentenza, avrebbe una portata più restrittiva di quella del principio previsto all’articolo 7, lettera f), della direttiva 95/46.

60      Infatti, mentre l’articolo 7, lettera f), si riferisce, in maniera generale, al «perseguimento dell’interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati», l’articolo 15 del TMG autorizzerebbe il fornitore di servizi a raccogliere e impiegare dati personali di un utente solamente nella misura in cui ciò sia necessario per consentire e fatturare l’effettiva fruizione dei media online. L’articolo 15 della TMG osterebbe quindi, in maniera generale, alla conservazione, al termine di una sessione di consultazione di media online, di dati personali per garantire la fruizione di tali media. Orbene, i servizi federali tedeschi che forniscono servizi di media online potrebbero altresì avere un interesse legittimo a garantire, al di là di ciascuna effettiva fruizione dei loro siti Internet accessibili al pubblico, la continuità del funzionamento di detti siti.

61      Come rilevato dall’avvocato generale ai paragrafi 100 e 101 delle sue conclusioni, una normativa nazionale siffatta non si limita a precisare, conformemente all’articolo 5 della direttiva 95/46, la nozione di «interesse legittimo» di cui all’articolo 7, lettera f), di tale direttiva.

62      A tale riguardo, occorre altresì ricordare che l’articolo 7, lettera f), della suddetta direttiva osta a che uno Stato membro escluda in modo categorico e generalizzato la possibilità che talune categorie di dati personali siano oggetto di trattamento, senza consentire la ponderazione dei diritti e degli interessi contrapposti in gioco nel caso specifico. Uno Stato membro non può quindi stabilire per tali categorie, in modo definitivo, il risultato della ponderazione dei diritti e degli interessi contrapposti, senza consentire un diverso risultato in ragione delle circostanze specifiche del caso concreto (v., in tal senso, sentenza del 24 novembre 2011, ASNEF e FECEMD, C‑468/10 e C‑469/10, EU:C:2011:777, punti 47 e 48).

63      Orbene, una normativa come quella di cui al procedimento principale riduce, con riferimento al trattamento di dati personali degli utenti di siti di media online, la portata del principio previsto all’articolo 7, lettera f), della direttiva 95/46, escludendo che l’obiettivo di garantire il funzionamento generale di tale medium online possa essere oggetto di ponderazione con l’interesse o i diritti e le libertà fondamentali di detti utenti, diritti e libertà che richiedono, conformemente alla disposizione in parola, tutela ai sensi dell’articolo 1, paragrafo 1, di tale direttiva.

64      Come risulta dall’insieme delle suesposte considerazioni, occorre rispondere alla seconda questione che l’articolo 7, lettera f), della direttiva 95/46 dev’essere interpretato nel senso che osta a una normativa di uno Stato membro ai sensi della quale un fornitore di servizi di media online può raccogliere e impiegare dati personali di un utente di tali servizi, in mancanza del suo consenso, solo nella misura in cui detta raccolta e detto impiego siano necessari per consentire e fatturare l’effettiva fruizione dei suddetti servizi da parte dell’utente in questione, senza che l’obiettivo di assicurare il funzionamento generale dei medesimi servizi possa giustificare l’impiego di tali dati dopo una sessione di consultazione degli stessi.

**Sulle spese**

65      Nei confronti delle parti nel procedimento principale la presente causa costituisce un incidente sollevato dinanzi al giudice nazionale, cui spetta quindi statuire sulle spese. Le spese sostenute da altri soggetti per presentare osservazioni alla Corte non possono dar luogo a rifusione.

Per questi motivi, la Corte (Seconda Sezione) dichiara:

**1)      L’articolo 2, lettera a), della direttiva 95/46 del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, dev’essere interpretato nel senso che un indirizzo di protocollo Internet dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di tale fornitore, un dato personale ai sensi di detta disposizione, qualora detto fornitore disponga di mezzi giuridici che gli consentano di far identificare la persona interessata grazie alle informazioni aggiuntive di cui il fornitore di accesso a Internet di detta persona dispone.**

**2)      L’articolo 7, lettera f), della direttiva 95/46 dev’essere interpretato nel senso che osta a una normativa di uno Stato membro ai sensi della quale un fornitore di servizi di media online può raccogliere e impiegare dati personali di un utente di tali servizi, in mancanza del suo consenso, solo nella misura in cui detta raccolta e detto impiego siano necessari per consentire e fatturare l’effettiva fruizione dei suddetti servizi da parte dell’utente in questione, senza che l’obiettivo di assicurare il funzionamento generale dei medesimi servizi possa giustificare l’impiego di tali dati dopo una sessione di consultazione degli stessi.**

**Autorità:** Cassazione civile sez. un.

**Data:** 27/12/2017

**n.** 30981

**Classificazioni:** PERSONA FISICA E DIRITTI DELLA PERSONALITÀ - Riservatezza (privacy) - - diritto di cronaca, di critica, di satira e diritto all'oblio

FATTI DI CAUSA

1. C.M., premesso di essere beneficiario dell'indennità riconosciutagli ex L. n. 210 del 1992, ha dedotto l'illegittima detenzione e divulgazione del dato sensibile relativo alle sue condizioni di salute derivante dall'indicazione nella causale di accredito dell'indennità "pagamento rateo arretrati bimestrali e posticipati (...) L. n. 210 del 1992". Ha indicato, come responsabili dell'uso e diffusione illegittima dei predetti dati sia la regione Campania, ente pubblico erogatore dell'indennità che il Banco di Napoli, essendo i ratei bimestrali accreditati su un suo conto corrente acceso presso l'istituto.

Ha chiesto, al riguardo, la rimozione del dato e il risarcimento del danno.

2. Il Tribunale di Napoli ha respinto la domanda sulla base delle seguenti argomentazioni:

- le condotte contestate sono quelle di illecita detenzione ed illecita diffusione del dato sensibile relativo alla salute del beneficiario decifrabile dall'indicazione della legge con la quale è stata riconosciuta l'indennità.

- i dati sensibili, secondo la definizione del D.Lgs. n. 196 del 2003, art. 4 sono dati personali idonei a rivelare lo stato di salute e la vita sessuale. Risulta incontestato che quelli in questione rientrino in tale categoria. I soggetti pubblici, diversi dagli enti pubblici economici, possono effettuare qualunque trattamento di dati sensibili anche senza il consenso dell'interessato ma solo per lo svolgimento delle funzioni istituzionali, se autorizzati da un'espressa previsione di legge e se perseguano finalità di rilevante interesse pubblico. Tra queste finalità rientrano senz'altro, perchè espressamente previste nel D.Lgs. n. 196 del 2003, art. 68 "le finalità di applicazione della disciplina in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni".

- i dati sensibili devono essere trattati secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato, laddove siano indispensabili per svolgere le attività istituzionali del soggetto pubblico e non possano essere eseguite mediante il trattamento di dati anonimi (art. 22, comma 3). In ogni caso i dati idonei a rivelare lo stato di salute non possono essere diffusi.

- Nel caso di specie, il riferimento, contenuto nella causale di accredito alla L. n. 210 del 1992 integra un dato sensibile che, alla luce del regime giuridico sopra indicato, non può essere diffuso dal soggetto pubblico e deve essere comunicato con modalità non esorbitanti rispetto alle finalità proprie dell'attività istituzionale svolta.

Al riguardo, il Tribunale ha evidenziato, da un lato, l'obbligo legislativo (R.D. n. 827 del 1924, art. 409) di specificare nei mandati di pagamento la precisa indicazione dell'oggetto di spesa; dall'altro la previsione contenuta nel D.Lgs. n. 196 del 2003, art. 22, comma 6, secondo la quale i dati sensibili devono essere trattati secondo tecniche di cifratura che li rendano inintelligibili.

- con riferimento all'illecito contestato alla Regione Campania, deve, in primo luogo, escludersi la diffusione dei dati in questione, in quanto gli stessi non sono stati portati a conoscenza di soggetti indeterminati. La trasmissione è avvenuta, mediante una rete informatica non accessibile a tutti, verso un soggetto determinato, quale è l'istituto di credito, a sua volta previamente autorizzato dal contratto di conto corrente intrattenuto con l'interessato e da ritenersi titolare del trattamento ovvero persona giuridica cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

- con riferimento all'istituto bancario, il tribunale ha rilevato che tra le modalità di trattamento così come descritte nell'art. 4 non c'è la mera detenzione. La condotta del Banco di Napoli si è risolta nell'esclusiva esecuzione di un obbligo contrattuale consistente nella descrizione, nell'estratto conto inviato al cliente, della causale del bonifico proveniente dalla Regione Campania. In questa condotta, non viene ravvisato alcun trattamento illecito dei dati sensibili in questione.

Anche in ordine all'istituto bancario s'impone, pertanto, il rigetto della domanda.

3. Avverso tale pronuncia ha proposto ricorso per cassazione C.M., affidato ad un unico complesso motivo. Hanno resisitito con controricorso la Regione Campania e la s.p.a Banco di Napoli.

4. La prima sezione, ravvisato un contrasto di giurisprudenza, ha richiesto la rimessione alle Sezioni Unite con l'ordinanza interlocutoria n. 3455 del 2017 nella quale si afferma:

5. Con decisione n. 10947 del 2014 la prima sezione della Corte di Cassazione in ricorso del tutto sovrapponibile a quello dedotto nel presente giudizio ha ritenuto che il riferimento all'indennità n. 210/92 contenesse un dato personale sensibile che l'ente pubblico avrebbe dovuto trattare, pur se autorizzato a farlo all'interno della sua attività istituzionale, con le cautele indicate dal D.Lgs. n. 196 del 2003, art. 22, comma 6. Il dato che la regione ha rivelato e la banca ha riportato riguarda direttamente l'informazione su un contagio dovuto a somministrazione di sangue o emoderivati o una menomazione permanente dovuta a vaccinazioni obbligatorie. Trattandosi di un dato relativo alla salute la cui diffusione è vietata, il trattamento poteva essere eseguito soltanto mediante tecniche di cifratura.

5.1 Con sentenza n. 10280 del 2015 la terza sezione civile della Corte ha adottato una soluzione opposta in fattispecie identica.

Le ragioni della decisione sono le seguenti:

a) la dizione "indennizzo ex lege n. 210 del 1992 inserita dalla regione Campania e dal Banco di Napoli nell'ordine di bonifico e nell'estratto conto non è un dato sensibile perchè può riferirsi non solo ai soggetti che hanno contratto le patologie ma anche ai congiunti delle persone decedute a causa dell'infezione derivante da trasfusione o vaccinazione.

b) Il dato non può dirsi diffuso in quanto non diretto a soggetti indeterminati ma ad una società per azioni designata dal soggetto cui il dato si riferisce. Non rende la comunicazione diffusione il fatto che la trasmissione sia diretta ad una persona giuridica, non potendo esigersi in questa ipotesi la preventiva identificazione della persona fisica cui indirizzare la comunicazione.

c) L'obbligo di cifratura riguarda soltanto i dati contenuti in banche dati o registri elettronici nonchè ai fini dell'interrogazione degli stessi da parte delle persone autorizzate ad accedervi. Invece nella specie la regione ha solo effettuato un pagamento ed indicato la causale.

d) La banca non ha l'obbligo della cifratura perchè è un soggetto privato.

e) Non costituisce violazione delle norme sulla riservatezza comunicare dati sensibili al rappresentante del titolare indicato proprio dal soggetto cui i dati si riferiscono come destinatario della comunicazione. Nella fattspecie la regione ha adempiuto ad obblighi di legge e la banca ad obblighi scaturenti da contratto.

f) La trasmissione dei dati dalla banca al cliente non costituisce neanche comunicazione e non costituisce comunicazione la trasmissione dei dati dalla regione alla banca perchè la banca non è altri che il mandatario con rappresentanza del correntista. Il pagamento (e i dati identificativi contenuti per eseguirlo) valgono come compiuti dal debitore direttamente al creditore.

g) Comunque la comunicazione sarebbe stata autorizzata dal R.D. n. 827 del 1924, art. 409 e dal D.Lgs. n. 267 del 2000, art. 185 nonchè dal Provvedimento del Garante per i dati personali n. 5 del 2009 che riguarda l'autorizzazione alle banche al trattamento dei dati personali per adempiere ad obblighi previdenziali.

**Diritto**
RAGIONI DELLA DECISIONE

6. Nell'unico motivo di ricorso viene, in primo luogo, dedotto che il Tribunale non ha colto la differenza cruciale, nell'ambito del sistema delineato dal D.Lgs. n. 196 del 2003, tra dato personale e dato sensibile, ed in particolare non ha rilevato che quest'ultimo attiene alla salute ed è conseguentemente soggetto ad una più intensa e peculiare disciplina di protezione anche quando il titolare sia un'autorità pubblica. In secondo luogo, viene evidenziato come nella pronuncia impugnata non venga compreso che la "detenzione" del dato è una categoria inapplicabile dovendo sostituirsi con il "trattamento". Il titolare del trattamento è tenuto a non ledere il diritto alla protezione dei dati personali anche in sede di uso e conservazione del dato non solo quando esso venga trasmesso.

6.1. Le cautele previste dal D.Lgs. n. 196 del 2003 operano anche quando il trattamento sia autorizzato dalla legge e sia rivolto alla realizzazione dell'attività istituzionale dell'ente pubblico. La ricorrenza di queste ultime condizioni non giustifica il trattamento e la trasmissione del dato in modo che sia del tutto riconoscibile l'identificazione dello stato di salute della ricorrente.

L'art. 22, comma 6, impone la cifratura dei dati sensibili, riferendosi specificamente a quelli di cui il soggetto pubblico sia autorizzato al trattamento anche senza il consenso dell'interessato. Pertanto, pur volendo applicare il R.D. n. 827 del 1924, art. 409, sarebbe stata comunque necessaria per la regione Campania, al fine di andare esente da responsabilità, la criptatura o cifratura del dato sensibile all'atto del trasferimento all'istituto di credito.

6.2. Per quanto riguarda la responsabilità dell'istituto di credito, la ricorrente evidenzia che la detenzione costituisce trattamento del dato sensibile ed è assoggettata alla tutela conseguente. Pertanto anche l'istituto di credito, ancorchè autorizzato al trattamento del dato, avrebbe dovuto "trattarlo" criptato essendo altrimenti conoscibile da parte di tutti gli impiegati della banca, dagli addetti al pagamento e da quelli che si occupano del recapito della posta.

Non elide l'obbligo di cifratura nè l'autorizzazione al pagamento nè il conferimento del mandato da parte del cliente ed il vincolo contrattuale assunto, certamente non diretto al trattamento contra legem dei propri dati sensibili.

Al contrario anche l'istituto di credito ha trattato il dato sensibile in dispregio del D.Lgs. n. 196 del 2003, art. 20 non adottando alcun accorgimento idoneo a renderlo non intellegibile ed inoltre Io ha diffuso illegittimamente consentendone una conoscenza estesa ad un grande numero di dipendenti.

Il dato infine è stato diffuso anche all'interno del circuito interbancario.

Non si riproducono le argomentazioni del ricorso rivolte al profilo risarcitorio in quanto la sentenza impugnata non le ha affrontate non riconoscendo il diritto azionato.

7. Come evidenziato nella sentenza impugnata, è necessario, per accertare se le condotte delle parti resistenti siano da qualificare illecite secondo i parametri stabiliti dal D.Lgs. n. 196 del 2003, verificare preliminarmente se i dati in questione siano personali ed in caso di risposta affermativa, se siano da qualificare sensibili; se l'utilizzazione degli stessi possa configurare un "trattamento" rilevante ai fini del sistema di protezione dei dati personali previsto dal nostro ordinamento ed infine se le parti resistenti siano identificabili come titolari del trattamento dei dati in questione.

7.1 Il primo interrogativo è di agevole soluzione: i dati desumibili dal richiamo alla L. n. 210 del 1992 sono personali in quanto relativi ad una persona fisica identificata (D.Lgs. n. 196 del 2003, art. 3, lett. b)) e sensibili perchè aventi un contenuto idoneo a rivelare lo stato di salute della persona identificata (D.Lgs. n. 196 del 2003, art. 3, lett. d)). Il regime di protezione dei dati sensibili relativi alla salute (e alla vita sessuale) è, come verrà evidenziato nell'illustrazione del quadro normativo, ispirato alla massima riservatezza dei dati stessi ed alla generale illiceità del trattamento di essi senza il consenso dell'interessato. Le eccezioni sono tassativamente predeterminante da norme legislative che ne procedimentalizzano puntualmente le modalità d'uso, specie se riguardanti dati sensibili non anonimi.

Deve, infine, essere precisato (come esattamente rilevato nell'ordinanza interlocutoria) che la dizione "pagamento rateo arretrati bimestrali e posticipati L. n. 210 del 1992" contiene la rivelazione del dato personale sensibile riguardante la salute del ricorrente in quanto la periodicità della corresponsione, desumibile inequivocamente dal testo come sopra descritto, non può che riguardare il soggetto affetto dalle patologie cui l'indennità si riferisce e non i suoi familiari-eredi ai quali la legge riconosce un importo a titolo di una tantum.

7.2 n secondo interrogativo si risolve con la definizione normativa del trattamento dei dati personali (nella specie sensibili) che consiste, D.Lgs. n. 196 del 2003, ex art. 4, lett. a), oltre alla raccolta e conservazione (ed alle forme di utilizzo connesse alla disponibilità dei dati stessi, come l'estrazione, la selezione, etc.), anche la comunicazione e la diffusione degli stessi. La comunicazione è l'operazione di trasmissione rivolta verso un soggetto determinato; la diffusione si rivolge verso un numero indeterminato di destinatari. Ne consegue che la trasmissione dei dati personali sensibili, della parte ricorrente, dalla regione Campania all'istituto bancario è esattamente riconducibile alla "comunicazione" ed è pertanto rientrante nella definizione normativa di "trattamento", così come lo sono le successive operazioni sui dati medesimi eseguite dal Banco di Napoli, in quanto riconducibili alla raccolta, selezione, e circolazione dei dati ovvero alle attività funzionali agli adempimenti contrttualmente richiesti, all'interno di una complessa organizzazione composta di un numero non esiguo ma determinato di addetti ed infine alla trasmissione al destinatario-ricorrente.

7.3 Il titolare del trattamento, D.Lgs. n. 196 del 2003, ex art. 4, lett. f) è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Dalle considerazioni svolte è del tutto agevole ritenere la regione Campania ed il Banco di Napoli titolari del trattamento dei dati sensibili del ricorrente ciascuno per le funzioni e gli adempimenti, rispettivamente di natura pubblica e contrattuale, posti in essere per pervenire all'accredito dell'indennità in favore dello stesso. Alle parti resistenti è, infatti, riconducibile il potere decisionale relativo alle modalità e agli strumenti utilizzati per il trattamento di tali dati.

8. Deve osservarsi che il sistema di protezione dei dati sensibili contenuto nel D.Lgs. n. 196 del 2003 si fonda sul principio generale della necessità del consenso espresso dell'interessato al trattamento di tali dati, in quanto dotati di uno rigoroso statuto normativo di garanzia della riservatezza, derogabile soltanto nelle ipotesi espressamente previste nella stessa legge o mediante diretta previsione normativa o mediante rinvio al potere conformativo-autorizzatorio del Garante.

Deve, pertanto, escludersi che il consenso al trattamento dei dati sensibili possa desumersi, in via indiretta da atti di natura diversa come la richiesta d'indennità ex L. n. 210 del 1992 o l'indicazione dell'istituto bancario presso il quale accreditare l'erogazione. L'esercizio di un diritto previsto dalla legge nei confronti dell'ente pubblico e l'attivazione di una delle prestazioni previste dal contratto di conto corrente di corrispondenza a carico dell'istituto bancario non modificano in alcun modo la posizione dei soggetti dei due rapporti giuridici dedotto in giudizio rispetto alla disciplina legislativa del trattamento dei dati sensibili. Il beneficiario dell'indennità è il soggetto interessato alla tutela dei propri dati sensibili e la regione Campania unitamente alla banca, sono i titolari del trattamento proprio perchè il vincolo assunto li porta ad avere la conoscenza e la disponibilità dei dati stessi. Non si può ritenere, di conseguenza, che l'interessato abbia, con le richieste inoltrate all'ente pubblico ed alla banca, autorizzato, in modo implicito, la comunicazione o la diffusione dei propri dati in quanto funzionale all'esercizio del diritto all'indennità e alla concreta erogazione del beneficio. Il rapporto giuridicamente qualificato sussistente tra soggetto titolare del diritto alla protezione dei propri dati sensibili e titolare del trattamento dei dati stessi è del tutto autonomo rispetto al vincolo legale o contrattuale che avvince, per ciò che concerne il diritto e l'erogazione dell'indennità, i soggetti obbligati e beneficiario. L'uno non confluisce nell'altro, mantenendo ciascuno di essi il proprio regime giuridico. Ci sono due relazioni produttive di effetti giuridici, l'una riguardante il beneficio accordato dalla L. n. 210 del 1992, l'altra la tutela del diritto fondamentale alla riservatezza in ordine ai dati personali relativi alla salute. Per questa seconda relazione giuridicamente qualificata che ha ad esclusivo oggetto il trattamento dei dati, la fonte di regolazione non può in alcun modo desumersi dal regime normativo e contrattuale dell'altra perchè si tratta di diritti e beni giuridici diversi e non sovrapponibili.

9. Dalle premesse svolte, risulta necessario, al fine di risolvere il contrasto di giurisprudenza prospettato dall'ordinanza interlocutoria n.3455 del 2017, illustrare il quadro normativo applicabile alla fattispecie dedotta in giudizio.

10. Prima di verificare come, all'interno del D.Lgs. n. 196 del 2003 operi la protezione dei dati sensibili anche nei confronti dei soggetti pubblici o privati che siano obbligati al trattamento per fini istituzionali o derivanti da vincolo negoziale con l'interessato, deve rilevarsi che la natura "super sensibile" dei dati personali connessi al riconoscimento dell'indennità in questione, è riconosciuto, in primo luogo, dalla stessa L. n. 210 del 1992. Nell'art. 3 è espressamente previsto che l'istruzione della domanda avvenga in modo da garantire "il diritto alla riservatezza anche mediante opportune modalità organizzative". (L. n. 210 del 1992, art. 3, comma 1). Nel successivo comma 1 bis la garanzia di riservatezza viene estesa a "chiunque nell'esercizio delle proprie funzioni venga a conoscenza" di persone danneggiate da complicanze di tipo irreversibile a causa di vaccinazioni obbligatorie, trasfusioni e somministrazioni di emoderivati. La norma si riferisce specificamente a tutti i soggetti che siano coinvolti per le funzioni svolte, dal titolare del trattamento dei dati (La USL), nell'istruzione e valutazione dell' istanza ed impone ad essi di rispettare il segreto d'ufficio e di adottare, nell'ambito delle proprie competenze, tutte le misure occorrenti per la tutela della riservatezza della persona interessata.

L'introduzione di una disciplina così puntuale in ordine alla tutela della riservatezza, non limitata all'affermazione del diritto, ma diretta in modo specifico ad imporre operativamente le cautele necessarie al titolare del trattamento ed a coloro che in ragione delle funzioni svolte ne vengano a conoscenza e a loro volta attuino il "trattamento" dei dati, non si rinviene nella formulazione originaria della norma risultando introdotto dopo l'entrata in vigore della prima disciplina normativa organica della tutela dei dati personali avvenuta con il D.Lgs. n. 675 del 1996. Il legislatore richiede "modalità organizzative" ovvero condotte positivamente rivolte a tutelare la riservatezza dei dati anche all'interno dell'articolazione strutturale e funzionale del soggetto pubblico, non limitandosi ad un richiamo alla non divulgabilità all'esterno dei dati conosciuti ed oggetto di trattamento.

Non se ne deve, conseguentemente, trascurare l'influenza ermeneutica nell'esame delle norme del D.Lgs. n. 196 del 2003, direttamente disciplinanti la fattispecie dedotta nel presente giudizio ed oggetto del contrasto di giurisprudenza illustrato nella parte narrativa della presente pronuncia.

11. E' utile precisare, preliminarmente, la collocazione delle norme nell'assetto sistematico del decreto legislativo. Esse si rinvengono nel capo II dal significativo titolo "regole ulteriori per i soggetti pubblici" che segue al capo I riguardante le "regole generali per il trattamento dei dati". Entrambi i capi sono contenuti nel Titolo 3^ che reca le "regole per tutti i trattamenti". La ripartizione normativa illustrata evidenzia la peculiarità del trattamento dei dati personali da parte dei soggetti pubblici e definisce l'ambito di derogabilità della regola generale del consenso dell'interessato al trattamento (D.Lgs. n. 196 del 2003, artt. 7 - 10).

L'art. 18 contiene le regole generali. Il trattamento dei dati personali è consentito ai soggetti pubblici solo nell'esercizio delle funzioni istituzionali ma devono essere osservati i presupposti ed i limiti previsti dal Codice (D.Lgs. n. 196 del 2003), dalla legge e dai regolamenti anche in relazione alla diversa natura dei dati. Entro questo duplice perimetro conformativo non è necessario il consenso dell'interessato.

Come indicato dalla norma di carattere generale, sopra esaminata, le disposizioni successive contengono una disciplina di dettaglio in ordine ai presupposti ed alle modalità di trattamento delle varie tipologie di dati. Per quanto riguarda specificamente i dati sensibili, l'art. 20 stabilisce che il trattamento dei dati sensibili da parte di un soggetto pubblico deve essere autorizzato da una espressa disposizione di legge nella quale siano specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. Ove la norma non contenga l'indicazione delle tipologie di dati da trattare e delle operazioni eseguibili ma individui il rilevante interesse pubblico posto a base del trattamento dei dati, è necessario che le specificazioni mancanti siano contenute in un atto regolamentare, adottato in conformità al parere del Garante. Ove neanche la finalità d'interesse pubblico sia espressa nella norma di legge, i soggetti pubblici possono chiedere al Garante l'individuazione delle attività che perseguano tali finalità e devono provvedere ad identificare e rendere pubblici i tipi di dati oggetto di trattamento. Sia nella prima che nella seconda ipotesi devono essere rispettate le modalità indicate nel successivo art. 22.

Come può agevolmente ricavarsi dall'esame dell'art. 20, il trattamento dei dati sensibili senza il consenso dell'interessato richiede che anche la predeterminazione normativa dei requisiti oggettivi entro i quali è consentito il predetto trattamento sia molto più specifica che per i dati personali non qualificabili come sensibili. Nessuna delle condizioni previste in via generale dall'art. 18 può essere desunta implicitamente dalle funzioni istituzionali del soggetto pubblico. E' necessario, invece, che sia la funzione istituzionale che le tipologie dei dati vengano individuate preventivamente e per quanto riguarda i tipi di dati anche rese pubbliche mediante atti normativi regolamentari assunti con la partecipazione vincolante del Garante. Il trattamento dei dati personali sensibili è rigidamente conformato dalle norme legislative e regolamentari che disciplinano in modo espresso i requisiti indefettibilmente richiesti.

Così come non può essere desunto implicitamente il consenso al trattamento dei dati sensibili da condotte diverse dall'adesione espressa dell'interessato, del pari la riserva di legge che giustifica il trattamento dei dati stessi da parte dei soggetti pubblici deve essere esplicita sia in ordine al rilevante interesse pubblico che alla predeterminazione dei dati trattabili, essendo altrimenti insufficiente a conferire, anche nell'ambito delle funzioni istituzionali del soggetto pubblico, il potere di trattare i dati sensibili senza il consenso dell'interessato.

Nella specie non è contestato che la regione Campania agisca non solo all'interno delle proprie attribuzioni istituzionali ma anche per una specifica finalità d'interesse pubblico direttamente desumibile dalla L. n. 210 del 1992.

L'art. 22 che detta i principi applicabili al trattamento dei dati sensibili e giudiziari, determina le "modalità organizzative" mediante le quali i dati in questione possono essere trattati, completando la disciplina legislativa relativa a(trattamento di tali dati con le prescrizioni relative al "come" procedere tutelando la riservatezza degli interessati.

In linea generale nel primo comma viene prescritto che i soggetti pubblici conformano il trattamento dei dati sensibili secondo modalità volta a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato (art. 22, comma 1). L'uso del predicato "conformano" richiama ed impone, al pari delle indicazioni normative sopra illustrate, condotte positivamente e specificamente rivolte alla protezione dei dati sensibili. Seguono le indicazioni di continenza nel trattamento dei dati sensibili da limitarsi, se se ne deve escludere la forma anonima, a quelli strettamente indispensabili alle finalità istituzionali da attuare (art. 22, commi 3 e 5), con divieto di utilizzazione di quelli superflui.

All'interno di questo rigoroso reticolo di regole di comportamento positivo si collocano le prescrizioni di centrale rilievo per l'esame delle questioni dedotte nel presente giudizio.

11.1 nell'art. 22, commi 6 e 7 viene espressamente imposto ai soggetti pubblici di trattare i dati relativi alla salute delle persone "con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessita".

Al riguardo deve rilevarsi che non è condivisibile l'interpretazione riduttiva che fornisce della norma la sentenza n. 10815 del 2015.

L'obbligo della cifratura o della criptatura non è limitato agli elenchi contenuti in elenchi, registri o banche dati, tenute con l'ausilio di strumenti elettronici, così come indicato nel comma 6 dell'art. 22 ma si estende a tutte le modalità di raccolta dei dati anche meramente cartacee come si ricava dalla più puntuale indicazione contenuta nel successivo comma 7, specificamente diretta ai dati sensibili relativi alla salute. In questa disposizione si precisa, infatti, che essi sono trattati con le modalità di cui al comma 6 (che richiede la cifratura o criptatura come illustrato) "anche quando sono tenuti in elenchi, registri, o banche di dati senza l'usilio di strumenti elettronici".

Il comma 8 contiene la norma di chiusura e stabilisce che i dati sensibili relative alla salute non possono essere diffusi.

Il quadro delineato evidenzia come il trattamento dei dati sensibili relativi alla salute deve indefettibilmente conformarsi a tutte le prescrizioni indicate nell'art. 22 e che si tratta di prescrizioni di natura inderogabile le quali non possono essere violate neanche ove non se ravvisi in concreto l'utilità o la necessità, essendo il sistema legislativo integrato di protezione dei dati sensibili ispirato al principio della massima limitazione possibile della circolazione e diffusione degli stessi senza il consenso dell'interessato. La tendenziale assolutezza del principio e la rigorosa definizione del perimetro autorizzatorio al trattamento di tali dati da parte dei soggetti pubblici induce ad escludere che residui in capo ai titolari, individuati D.Lgs. n. 196 del 2003, ex art. 18 e ss. alcun potere discrezionale in ordine all'adempimento delle prescrizioni normative relative al trattamento. L'art. 22 ne impone la continenza e la criptatura o cifratura, senza alcun margine di apprezzamento relativo alla efficacia dello strumento in ordine al concreto uso del dato.

12. Non può, pertanto, che darsi continuità all'orientamento espresso dalla sentenza della prima sezione civile n. 10947 del 2014, e ritenere che la regione Campania fosse tenuta in ogni operazione qualificabile come trattamento dei dati, D.Lgs. n. 196 del 2003, ex art. 4, lett. a), ad osservare le prescrizioni puntuali contenute nell'art. 22, comma 6 e, conseguentemente ad adottare tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessita. Non soltanto la trasmissione mediante comunicazione (come nella specie) o diffusione dei dati relativi alla salute ma anche la raccolta, la conservazione e l'estrazione e selezione degli stessi deve avvenire mediante codici cifrati e criptati per impedirne la potenzialità diffusiva, limitando l'identificazione degli interessati alle operazioni strettamente necessarie allo scopo finale dell'erogazione dell'indennità.

13. Tale orientamento, coerente con la lettera e la ratio della disciplina legislativa esaminata, non è in contrasto con gli obblighi di trasparenza posti a carico della pubblica amministrazione nell'allocazione e distribuzione delle risorse finanziarie ai quali i soggetti pubblici sono tenuti nei confronti degli organi di controllo, nei confronti dei terzi interessati e più in generale verso i cittadini e gli utenti perchè i beneficiari dell'indennità sono identificabili per relationem per mezzo dei codici cifrati o criptati limitatamente però a cio che è strettamente necessario a provvedere alle erogazioni ed a rispettare gli altri obblighi normativi ed istituzionali. All'interno delle articolazioni organizzative del soggetto pubblico le operazioni di trattamento dei dati, ovvero la conservazione, l'estrazione e la selezione di essi devono avvenire mediante tecniche che non consentano l'individuazione del soggetto o escludano il collegamento degli elementi identificativi soggettivi con il dato relativo alla salute. Le operazioni di trasmissione e comunicazione, infine, devono essere corredate delle medesime cautele in considerazione della maggiore esposizione al rischio della conoscenza non consentita dei dati in questione in queste specifiche tipologie di trattamento.

14. La soluzione adottata in ordine al soggetto pubblico titolare del trattamento, deve essere estesa anche all'istituto bancario, anch'esso qualificabile, come già illustrato, quale titolare del trattamento, in quanto tenuto alla raccolta, conservazione e comunicazione agli interessati dei dati medesimi.

14.1. Al riguardo, deve rilevarsi preliminarmente che il regime derogatorio contenuto nel D.Lgs. n. 196 del 2003, art. 18 e ss. non trova diretta applicazione nei confronti dell'istituto bancario, trattandosi di persona giuridica di diritto privato. Non incide su tale qualificazione e sul regime giuridico applicabile il fatto che l'accredito dell'indennità costituisca la fase finale di un procedimento a formazione progressiva volto alla realizzazione di una finalità di rilevante interesse pubblico.

14.2 Il D.Lgs. n. 196 del 2003 contiene, infatti, un'autonoma regolamentazione per i soggetti privati e gli enti pubblici economici nel capo 3, del titolo 3 (artt. da 23 a 27) notevolmente diversa da quella contenuta nel capo 2 e riferita ai soggetti pubblici.

Nell'art. 23 è contenuta la regola generale della necessità del consenso espresso dell'interessato reso per iscritto se relativo a dati sensibili ed avente ad oggetto la chiara individuazione della o delle tipologie di trattamento.

L'art. 24 esclude la necessità del consenso per adempiere ad obblighi normativi o contrattuali o in altre ipotesi elencate dalla norma ma non riguardanti i dati sensibili. Per questi ultimi, l'art. 26 richiede sempre il consenso scritto dell'interessato e l'autorizzazione preventiva del Garante (art. 26, comma 1). Il comma 4 della norma prevede un elenco di attività per le quali, ferma la previa autorizzazione del Garante, non è necessario lo specifico consenso scritto. Nella sentenza n.10280 del 2015 e nella prospettazione difensiva delle parti controricorrenti si è ritenuta applicabile alla fattispecie dedotta nel presente giudizio la deroga prevista nell'art. 26, comma 4, lett. D inferendo dalla non necessità del consenso la superfluita della cifratura o criptatura. La disposizione invocata fa riferimento al trattamento dei dati sensibili necessario per l'adempimento di obblighi normativi riguardanti "la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza".

14.3 Al riguardo, pur rientrando l'indennità in oggetto nelle prestazioni in senso lato previdenziali ed assistenziali, deve ritenersi ai fini dell'applicabilità della norma, la necessità che vi sia un nesso funzionale con il rapporto di lavoro come si rileva dalla esegesi testuale della norma.

La prestazione derivante dall'applicabilità della L. n. 210 del 1992 è estranea al complesso di obblighi e benefici che derivano dal rapporto di lavoro. Con riferimento ai dati sensibili ad essa riconducibili, è necessario in linea generale il consenso espresso dell'interessato ex art. 26, comma 1.

14.4 Peraltro, pur volendo ritenere autonomo il riferimento alle prestazioni previdenziali ed assistenziali, deve escludersi che l'istituto bancario non sia tenuto al trattamento dei dati in modo da occultarne la riconoscibilità all'interno della propria struttura organizzativa, oltre che nella eventuale trasmissione a soggetti determinati o nella diffusione.

15. L'interpretazione sistematica delle norme di protezione dei dati sensibili, contenute nel D.Lgs. n. 196 del 2003, porta ad escludere che le cautele poste a carico del soggetto pubblico non debbano essere applicate anche ai soggetti privati cui i dati siano trasmessi in virtù di un obbligo legale o di un vincolo contrattuale, al fine di completare il procedimento di riconoscimento ed erogazione dell'indennità. Diversamente ragionando si determinerebbe un vulnus privo di ragionevolezza in ordine al trattamento dei dati nella fase, successiva alla trasmissione di essi all'istituto bancario, caratterizzata dal potenziale aumento del numero dei soggetti che ne possono venire a contatto. Le cautele della cifratura e della criptatura sono finalizzate proprio ad evitare la conoscenza dei dati sensibili attinenti alla salute da parte di soggetti che ne possano venire a contatto per l'inclusione nelle organizzazioni complesse titolari del trattamento e, conseguentemente possano estrarli, selezionarli, farne uso e diffonderne il contenuto. Il legislatore sia nel D.Lgs. n. 196 del 2003, in linea generale, che nella L. n. 210 del 1992, ha voluto cercare di limitare al massimo il pericolo connesso alla conoscenza dei dati relativi alla salute in quanto "super sensibili", indicando modalità di trattamento che nascondano l'identificazione dei soggetti portatori di patologie fisiche o psichiche salvo che per l'esecuzione dell'attività inevitabilmente necessaria alla realizzazione della finalità d'interesse pubblico o per l'adempimento degli obblighi contrattualmente assunti.

15.1 Al riguardo anche l'autorizzazione del Garante n. 5 del 2009, avente ad oggetto le modalità di trattamento dei dati sensibili senza il consenso dell'interessato da parte delle imprese bancarie per l'attuazione degli obblighi contrattuali assunti, prescrive preventivamente che "prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice".

Nel punto n. 2, del Capo 6, dell'Autorizzazione del Garante sopra indicata, riguardante le "prescrizioni comuni a tutti i trattamenti" viene infine prescritto che il trattamento dei dati sensibili deve essere effettuato con operazioni nonchè con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto alle finalità perseguite, dovendosi altresì rispettare quanto stabilito nell'Autorizzazione n. 2 del 2009. Quest'ultima Autorizzazione, riguardante il trattamento dei dati relativi alla salute e alla vita sessuale è interamente finalizzata a prescrivere comportamenti e modalità organizzative ispirate alla massima riservatezza in ordine al trattamento complessivo dei dati sensibili.

16. Pertanto, deve ritenersi esteso, per le ragioni complessivamente svolte, anche all'istituto bancario l'obbligo di procedere al trattamento dei dati sensibili dei propri clienti titolari dell'indennità attribuita ex lege n. 210 del 1992 mediante tecniche che non ne consentano l'identificazione.

17. In conclusione, il soggetto pubblico - Regione Campania - ed il soggetto persona giuridica privata - Banco di Napoli - sono tenuti, in qualità di titolari del trattamento dei dati personali del ricorrente, nel procedimento di riconoscimento, erogazione e concreto accredito dell'indennità ex lege n. 210 del 1992, ad occultare, mediante tecniche di cifratura o criptatura, il riferimento alla legge sopra indicata, in quanto rivelatore dello stato di salute del beneficiario dell'indennità. Le modalità organizzative, rimesse ai titolari del trattamento dei dati, devono essere dirette ad escludere il collegamento tra il dato sensibile e il soggetto beneficiario dell'indennità ed a limitare alle operazioni indispensabili ed ai soli addetti a tali specifiche operazioni la conoscenza del dato, celandone ai restanti componenti delle due organizzazioni complesse la decifrabilità ed, infine, conservando le medesime cautele nella comunicazione dei dati.

18. L'unico motivo di ricorso deve, in conclusione, essere accolto e la sentenza cassata con rinvio al tribunale di Napoli in diversa composizione perchè si attenga al seguente principio di diritto: I dati sensibili idonei a rivelare lo stato di salute possono essere trattati soltanto mediante modalità organizzative, quali tecniche di cifratura o criptatura che rendono non identificabile l'interessato. Ne consegue che i soggetti pubblici o le persone giuridiche private, anche quando agiscano rispettivamente in funzione della realizzazione di una finalità di pubblico interesse o in adempimento di un obbligo contrattuale, sono tenuti all'osservanza delle predette cautele nel trattamento dei dati in questione".

La novità della questione impone la compensazione delle spese del presente giudizio.

**PQM**
P.Q.M.

Accoglie il ricorso. Cassa la sentenza impugnata e rinvia al Tribunale di Napoli in diversa persona.