Raccolta della giurisprudenza

SENTENZA DELLA CORTE (Grande Sezione)

20 settembre 2022 *

«Rinvio pregiudiziale – Mercato unico dei servizi finanziari – Abusi di mercato – Abuso di informazioni privilegiate – Direttiva 2003/6/CE – Articolo 12, paragrafo 2, lettere a) e d) – Regolamento (UE) n. 596/2014 – Articolo 23, paragrafo 2, lettere g) e h) – Poteri di vigilanza e di indagine dell'Autorità dei mercati finanziari (AMF) – Obiettivo di interesse generale volto a tutelare l'integrità dei mercati finanziari dell'Unione europea e la fiducia del pubblico negli strumenti finanziari – Possibilità per l'AMF di chiedere le registrazioni di dati relativi al traffico detenuti da un operatore di servizi di comunicazione elettronica – Trattamento dei dati personali nel settore delle comunicazioni elettroniche – Direttiva 2002/58/CE – Articolo 15, paragrafo 1 – Carta dei diritti fondamentali dell'Unione europea – Articoli 7, 8 e 11 nonché articolo 52, paragrafo 1 – Riservatezza delle comunicazioni – Limitazioni – Normativa che prevede la conservazione generalizzata e indiscriminata dei dati relativi al traffico da parte degli operatori di servizi di comunicazione elettronica – Possibilità per un giudice nazionale di limitare gli effetti nel tempo di una declaratoria di invalidità di disposizioni legislative nazionali incompatibili con il diritto dell'Unione – Esclusione»

Nelle cause riunite C-339/20 e C-397/20,

aventi ad oggetto le domande di pronuncia pregiudiziale proposte alla Corte, ai sensi dell'articolo 267 TFUE, dalla Cour de cassation (Corte di cassazione, Francia), con decisioni del 1º aprile 2020, pervenute in cancelleria, rispettivamente, il 24 luglio 2020 e il 20 agosto 2020, nei procedimenti penali a carico di

**VD** (C-339/20),

**SR** (C-397/20),

LA CORTE (Grande Sezione),

composta da K. Lenaerts, presidente, A. Arabadjiev, A. Prechal, S. Rodin, I. Jarukaitis e I. Ziemele, presidenti di sezione, T. von Danwitz, M. Safjan, F. Biltgen, P.G. Xuereb (relatore), N. Piçarra, L.S. Rossi e A. Kumin, giudici,

avvocato generale: M. Campos Sánchez-Bordona

cancelliere: R. Şereş, amministratrice

vista la fase scritta del procedimento e in seguito all'udienza del 14 settembre 2021,

* Lingua processuale: il francese.

considerate le osservazioni presentate:

– per VD, da D. Foussard e F. Peltier, avocats;

– per SR, da M. Chavannes e P. Spinosi, avocats;

– per il governo francese, da A. Daniel, E. de Moustier, D. Dubois, J. Illouz e T. Stéhelin, in qualità di agenti;

– per il governo danese, par N. Holst-Christensen, N. Lykkegaard e M. Søndahl Wolff, in qualità di agenti;

– per il governo estone, da A. Kalbus e M. Kriisa, in qualità di agenti;

– per l'Irlanda, da M. Browne, A. Joyce e J. Quaney, in qualità di agenti, assistiti da D. Fennelly, BL;

– per il governo spagnolo, da L. Aguilera Ruiz, in qualità di agente;

– per il governo polacco, da B. Majczyna, in qualità di agente;

– per il governo portoghese, da P. Barros da Costa, L. Inez Fernandes, L. Medeiros e I. Oliveira, in qualità di agenti;

– per la Commissione europea, da S.L. Kalėda, H. Kranenborg, T. Scharf e F. Wilman, in qualità di agenti;

– per il Garante europeo della protezione dei dati, da A. Buchta, M. Guglielmetti, C.-A. Mamier e D. Nardi, in qualità di agenti,

sentite le conclusioni dell'avvocato generale, presentate all'udienza del 18 novembre 2021,

ha pronunciato la seguente

## Sentenza

1 Le domande di pronuncia pregiudiziale vertono, in sostanza, sull'interpretazione dell'articolo 12, paragrafo 2, lettere a) e d), della direttiva 2003/6/CE del Parlamento europeo e del Consiglio, del 28 gennaio 2003, relativa all'abuso di informazioni privilegiate e alla manipolazione del mercato (abusi di mercato) (GU 2003, L 96, pag.16) e dell'articolo 23, paragrafo 2, lettere g) e h), del regolamento (UE) n. 596/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, relativo agli abusi di mercato (regolamento sugli abusi di mercato) e che abroga la direttiva 2003/6/CE del Parlamento europeo e del Consiglio e le direttive 2003/124/CE, 2003/125/CE e 2004/72/CE della Commissione (GU 2014, L 173, pag. 1), in combinato disposto con l'articolo 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU 2002, L 201, pag. 37), come modificata dalla direttiva 2009/136/CE del

Parlamento europeo e del Consiglio, del 25 novembre 2009 (GU 2009, L 337, pag. 11) (in prosieguo: la «direttiva 2002/58»), letti alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»).

2 Tali domande sono state presentate nell'ambito dei procedimenti penali instaurati a carico di VD e di SR per i reati di abuso di informazioni privilegiate, di abuso secondario di informazioni privilegiate, di favoreggiamento, di corruzione e di riciclaggio.

## Contesto normativo

### *Diritto dell'Unione*

*Direttiva 2002/58*

3 I considerando 2, 6, 7 e 11 della direttiva 2002/58 così recitano:

«(2) La presente direttiva mira a rispettare i diritti fondamentali e si attiene ai principi riconosciuti in particolare dalla [Carta]. In particolare, la presente direttiva mira a garantire il pieno rispetto dei diritti di cui agli articoli 7 e 8 di tale Carta.

(...)

(6) L'Internet ha sconvolto le tradizionali strutture del mercato fornendo un'infrastruttura mondiale comune per la fornitura di un'ampia serie di servizi di comunicazione elettronica. I servizi di comunicazione elettronica accessibili al pubblico attraverso l'Internet aprono nuove possibilità agli utenti ma rappresentano anche nuovi pericoli per i loro dati personali e la loro vita privata.

(7) Nel settore delle reti pubbliche di comunicazione occorre adottare disposizioni legislative, regolamentari e tecniche specificamente finalizzate a tutelare i diritti e le libertà fondamentali delle persone fisiche e i legittimi interessi delle persone giuridiche, con particolare riferimento all'accresciuta capacità di memorizzazione e trattamento dei dati relativi agli abbonati e agli utenti.

(...)

(11) La presente direttiva, analogamente alla 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)], non affronta le questioni relative alla tutela dei diritti e delle libertà fondamentali inerenti ad attività che non sono disciplinate dal diritto comunitario. Lascia pertanto inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti di cui all'articolo 15, paragrafo 1, della presente direttiva, necessari per tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) e l'applicazione della legge penale. Di conseguenza, la presente direttiva non pregiudica la facoltà degli Stati membri di effettuare intercettazioni legali di comunicazioni elettroniche o di prendere altre misure, se necessario, per ciascuno

di tali scopi e conformemente alla Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali, [firmata a Roma il 4 novembre 1950] come interpretata dalle sentenze della Corte europea dei diritti dell'uomo. Tali misure devono essere appropriate, strettamente proporzionate allo scopo perseguito, necessarie in una società democratica ed essere soggette ad idonee garanzie conformemente alla precitata Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali».

4 L'articolo 1 della direttiva 2002/58, intitolato «Finalità e campo d'applicazione», così dispone:

«1. La presente direttiva prevede l'armonizzazione delle disposizioni nazionali necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata e alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno della Comunità.

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

3. La presente direttiva non si applica alle attività che esulano dal campo di applicazione del [Trattato FUE], quali quelle disciplinate dai titoli V e VI del [Trattato UE] né, comunque, alle attività riguardanti la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) o alle attività dello Stato in settori che rientrano nel diritto penale».

5 L'articolo 2 della direttiva in questione, intitolato «Definizioni», al secondo comma, lettera b), prevede quanto segue:

«Si applicano (...) le seguenti definizioni:

(...)

b) "dati relativi al traffico": qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione».

6 Ai sensi dell'articolo 5 della medesima direttiva, intitolato «Riservatezza delle comunicazioni»:

«1. Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare essi vietano l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell'articolo 15, paragrafo 1. Questo paragrafo non impedisce la memorizzazione tecnica necessaria alla trasmissione della comunicazione fatto salvo il principio della riservatezza.

2. Il paragrafo 1 non pregiudica la registrazione legalmente autorizzata di comunicazioni e dei relativi dati sul traffico se effettuata nel quadro di legittime prassi commerciali allo scopo di fornire la prova di una transazione o di una qualsiasi altra comunicazione commerciale.

3. Gli Stati membri assicurano che l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, a norma della direttiva [95/46], tra l'altro sugli scopi del trattamento. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio».

7 L'articolo 6 della direttiva 2002/58, intitolato «Dati sul traffico», stabilisce quanto segue:

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

2. I dati relativi al traffico che risultano necessari ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione possono essere sottoposti a trattamento. Tale trattamento è consentito solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento.

3. Ai fini della commercializzazione dei servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha facoltà di sottoporre a trattamento i dati di cui al paragrafo 1 nella misura e per la durata necessaria per siffatti servizi, o per la commercializzazione, sempre che l'abbonato o l'utente a cui i dati si riferiscono abbia espresso preliminarmente il proprio consenso. Gli abbonati o utenti hanno la possibilità di ritirare il loro consenso al trattamento dei dati relativi al traffico in qualsiasi momento.

(...)

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

(...)».

8 L'articolo 9 di tale direttiva, intitolato «Dati relativi all'ubicazione diversi dai dati relativi al traffico», al paragrafo 1 prevede quanto segue:

«Se i dati relativi all'ubicazione diversi dai dati relativi al traffico, relativi agli utenti o abbonati di reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico[,] possono essere sottoposti a trattamento, essi possono esserlo soltanto a condizione che siano stati resi anonimi o che l'utente o l'abbonato abbiano dato il loro consenso, e sempre nella misura e per la durata necessaria per la fornitura di un servizio a valore aggiunto. Prima di chiedere il loro consenso, il fornitore del servizio deve informare gli utenti e gli abbonati sulla natura dei dati relativi

all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti a trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto. (...)».

9 L'articolo 15 della direttiva 2002/58, intitolato «Applicazione di alcune disposizioni della direttiva [95/46]», al paragrafo 1 così recita:

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

*Direttiva 2003/6*

10 I considerando 1, 2, 12, 37, 41 e 44 della direttiva 2003/6 sono del seguente tenore:

«(1) Un autentico mercato unico dei servizi finanziari è cruciale per la crescita economica e la creazione di posti di lavoro nella Comunità.

(2) Un mercato finanziario integrato ed efficiente non può esistere senza che se ne tuteli l'integrità. Il regolare funzionamento dei mercati mobiliari e la fiducia del pubblico nei mercati costituiscono fattori essenziali di crescita e di benessere economico. Gli abusi di mercato ledono l'integrità dei mercati finanziari e compromettono la fiducia del pubblico nei valori mobiliari e negli strumenti derivati.

(...)

(12) Gli abusi di mercato comprendono l'abuso di informazioni privilegiate e la manipolazione del mercato. La normativa contro l'abuso di informazioni privilegiate persegue lo stesso obiettivo della normativa contro la manipolazione del mercato: assicurare l'integrità dei mercati finanziari comunitari e accrescere la fiducia degli investitori nei mercati stessi. (...)

(...)

(37) Il conferimento all'autorità competente di ogni Stato membro di un insieme minimo comune di strumenti e poteri forti garantirà l'efficacia della sua opera di vigilanza. I gestori di mercato e tutti gli operatori economici dovrebbero parimenti contribuire, ai rispettivi livelli, all'integrità del mercato. (...)

(...)

(41) Poiché l'obiettivo delle misure proposte, vale a dire prevenire gli abusi di mercato sotto forma di abuso di informazioni privilegiate e di manipolazione del mercato, non può essere sufficientemente realizzato dagli Stati membri e può dunque, a motivo delle dimensioni e degli effetti dell'azione in questione, essere realizzato meglio a livello comunitario, la Comunità può intervenire, in base al principio di sussidiarietà sancito dall'articolo 5 [TUE]. La presente direttiva si limita a quanto necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(44) La presente direttiva rispetta i diritti fondamentali e osserva i principi riconosciuti segnatamente dalla [Carta], in particolare l'articolo 11, nonché l'articolo 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. (...)».

11 L'articolo 11 di tale direttiva così dispone:

«Fatte salve le competenze delle autorità giudiziarie, ogni Stato membro designa un'unica autorità amministrativa competente a vigilare sull'applicazione delle disposizioni adottate ai sensi della presente direttiva.

(...)».

12 Ai sensi dell'articolo 12 della medesima direttiva:

«1. All'autorità competente sono conferiti tutti i poteri di vigilanza e di indagine necessari per l'esercizio delle sue funzioni. (...)

2. Fatto salvo l'articolo 6, paragrafo 7, i poteri di cui al paragrafo 1 del presente articolo sono esercitati in conformità della legislazione nazionale e includono almeno il diritto di:

a) avere accesso a qualsiasi documento sotto qualsiasi forma e ottenerne copia;

(...)

d) richiedere le registrazioni telefoniche esistenti e le informazioni esistenti relative al traffico;

(...)».

*Regolamento n. 596/2014*

13 Il regolamento n. 596/2014 ha abrogato e sostituito la direttiva 2003/6 con effetto dal 3 luglio 2016.

14 I considerando 1, 2, 7, 24, 44, 62, 65, 66, 77 e 86 di tale regolamento sono del seguente tenore:

«(1) Un autentico mercato interno dei servizi finanziari è di importanza fondamentale per la crescita economica e la creazione di posti di lavoro nell'Unione.

(2) Un mercato finanziario integrato, efficiente e trasparente non può esistere senza che se ne tuteli l'integrità. Il regolare funzionamento dei mercati mobiliari e la fiducia del pubblico nei mercati costituiscono fattori essenziali di crescita e di benessere economico. Gli abusi di mercato ledono l'integrità dei mercati finanziari e compromettono la fiducia del pubblico nei valori mobiliari e negli strumenti derivati.

(...)

(7) Abuso di mercato è il concetto che comprende le condotte illecite nei mercati finanziari e ai fini del presente regolamento dovrebbe essere inteso come abuso di informazioni privilegiate, comunicazione illecita di informazioni privilegiate e manipolazione del mercato. Tali condotte impediscono una piena ed effettiva trasparenza del mercato, che è un requisito fondamentale affinché tutti gli attori economici siano in grado di operare su mercati finanziari integrati.

(...)

(24) Quando una persona fisica o giuridica che detiene informazioni privilegiate acquisisce o cede, o tenta di acquisire o di cedere, per conto proprio o per conto di terzi, direttamente o indirettamente, strumenti finanziari cui le informazioni si riferiscono, dovrebbe essere implicito che tale persona abbia utilizzato tali informazioni. Tale presunzione non pregiudica i diritti della difesa. La questione di sapere se una persona abbia violato il divieto di abuso di informazioni privilegiate o tentato di abusare di informazioni privilegiate dovrebbe essere analizzata alla luce delle finalità del presente regolamento, che è quella di tutelare l'integrità del mercato finanziario e rafforzare la fiducia degli investitori, la quale si fonda, a sua volta, sulla garanzia che gli investitori siano posti su un piano di parità e tutelati dall'abuso di informazioni privilegiate.

(...)

(44) I prezzi di numerosi strumenti finanziari sono fissati con riferimento a indici di riferimento (benchmarks). La manipolazione o tentata manipolazione degli indici di riferimento, compresi i tassi dei prestiti interbancari, può avere conseguenze gravi per la fiducia dei mercati e potrebbe determinare perdite consistenti per gli investitori oppure distorsioni nell'economia reale. (...)

(62) Il conferimento all'autorità competente di ogni Stato membro di una serie di strumenti, poteri e risorse adeguati garantirà l'efficacia della sua opera di vigilanza. Di conseguenza, il presente regolamento prevede, in particolare, una serie minima di poteri di vigilanza e di indagine che dovrebbero essere conferiti alle autorità competenti degli Stati membri conformemente al diritto nazionale. Tali poteri dovrebbero essere esercitati, ove il diritto nazionale lo richieda, previa richiesta alle competenti autorità giudiziarie. (...)

(...)

(65) Le registrazioni di conversazioni telefoniche e i tabulati concernenti il traffico dati esistenti presso le società d'investimento, gli enti creditizi e istituzioni finanziarie che eseguono operazioni e ne documentano l'esecuzione, nonché i tabulati relativi al traffico telefonico e di dati esistenti presso gli operatori di telecomunicazioni[,] costituiscono elementi di prova indispensabili, e a volte gli unici elementi di prova disponibili, per individuare e dimostrare

l'esistenza dell'abuso di informazioni privilegiate e di manipolazione del mercato. I tabulati relativi al traffico telefonico e di dati possono determinare l'identità del responsabile della diffusione di informazioni false o fuorvianti, o stabilire che sono intervenuti contatti tra alcune persone per un certo periodo e che due o più persone sono in relazione fra loro. Pertanto, le autorità competenti dovrebbero avere la possibilità di richiedere le registrazioni delle conversazioni telefoniche e delle comunicazioni elettroniche e i tabulati relativi al traffico dati detenuti da una società di investimento, da un ente creditizio o da un'altra istituzione finanziaria conformemente alla direttiva 2014/65/UE [del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE (GU 2014, L 173, pag. 349)]. L'accesso ai tabulati relativi al traffico telefonico e di dati è necessario a fini probatori e investigativi in ordine a possibili casi di abuso di informazioni privilegiate e di manipolazione del mercato e, quindi, per individuare e irrogare sanzioni per gli abusi di mercato. Allo scopo di introdurre pari condizioni nell'Unione in relazione all'accesso ai tabulati esistenti relativi al traffico telefonico e di dati detenuti da un operatore di telecomunicazioni o ai dati esistenti relativi al traffico telefonico e ai tabulati relativi al traffico dati detenuti da una società di investimento, un ente creditizio o un'istituzione finanziaria, le autorità competenti dovrebbero, conformemente al diritto nazionale, essere in grado di chiedere i tabulati esistenti relativi al traffico telefonico e di dati detenuti da un operatore di telecomunicazioni nella misura in cui il diritto nazionale lo consenta, e le registrazioni esistenti di conversazioni telefoniche e i tabulati relativi al traffico dati detenuti da una società di investimento, nei casi in cui esista un ragionevole sospetto che tali registrazioni o tabulati connessi all'oggetto dell'ispezione o dell'indagine possano essere rilevanti al fine di dimostrare l'abuso di informazioni privilegiate o la manipolazione del mercato che violino il presente regolamento. L'accesso ai tabulati relativi al traffico telefonico e di dati detenuti da un operatore di telecomunicazioni non include l'accesso al contenuto delle comunicazioni telefoniche vocali.

(66) Se il presente regolamento specifica una serie minima di poteri che dovrebbero essere conferiti alle autorità competenti, tali poteri devono essere esercitati nell'ambito di un sistema giuridico nazionale completo che garantisca il rispetto dei diritti fondamentali, compreso il diritto alla tutela della vita privata. Per esercitare tali poteri, che possono portare a gravi interferenze con il diritto alla tutela per la vita privata e familiare, il domicilio e le comunicazioni, gli Stati membri dovrebbero disporre di garanzie adeguate ed efficaci contro ogni abuso, a[d] esempio un requisito per ottenere, se necessario, un'autorizzazione preventiva da parte delle autorità giudiziarie dello Stato membro interessato. Gli Stati membri dovrebbero prevedere la possibilità che le autorità competenti esercitino tali poteri invasivi nella misura necessaria per indagare correttamente su casi gravi in assenza di mezzi equivalenti per conseguire in modo efficace lo stesso risultato.

(...)

(77) Il presente regolamento rispetta i diritti fondamentali e osserva i principi riconosciuti dalla [Carta]. Il presente regolamento dovrebbe quindi essere interpretato e applicato conformemente a tali diritti e principi. (...)

(...)

(86) Poiché l'obiettivo del presente regolamento, vale a dire prevenire gli abusi di mercato sotto forma di abuso di informazioni privilegiate, comunicazione illecita di informazioni privilegiate e di manipolazione del mercato, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo della sua portata e dei suoi effetti, può essere conseguito meglio a livello dell'Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 [TUE]. Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo».

15 Ai sensi dell'articolo 1 di detto regolamento:

«Il presente regolamento istituisce un quadro normativo comune in materia di abuso di informazioni privilegiate, comunicazione illecita di informazioni privilegiate e manipolazione del mercato (abusi di mercato), nonché misure per prevenire gli abusi di mercato, onde garantire l'integrità dei mercati finanziari dell'Unione e accrescere la tutela degli investitori e la fiducia in tali mercati».

16 L'articolo 3 del medesimo regolamento, intitolato «Definizioni», al paragrafo 1, punto 27, così dispone:

«Ai fini del presente regolamento si intende per:

(...)

27) "registrazioni di dati relativi al traffico": registrazioni di dati relativi al traffico, quali definite nell'articolo 2, secondo comma, lettera b), della direttiva [2002/58]».

17 Ai sensi dell'articolo 14 del regolamento n. 596/2014, intitolato «Divieto di abuso di informazioni privilegiate e di comunicazione illecita di informazioni privilegiate»:

«Non è consentito:

a) abusare o tentare di abusare di informazioni privilegiate;

b) raccomandare ad altri di abusare di informazioni privilegiate o indurre altri ad abusare di informazioni privilegiate; oppure

c) comunicare in modo illecito informazioni privilegiate».

18 L'articolo 22 di tale regolamento prevede quanto segue:

«Fatte salve le competenze delle autorità giudiziarie, ogni Stato membro designa un'unica autorità amministrativa competente ai fini del presente regolamento. (...)».

19 L'articolo 23 di detto regolamento, intitolato «Poteri delle autorità competenti», ai paragrafi 2 e 3 così dispone:

«2. Per adempiere ai compiti loro assegnati dal presente regolamento, le autorità competenti dispongono almeno, conformemente al diritto nazionale, dei seguenti poteri di controllo e di indagine:

a) di accedere a qualsiasi documento e a dati sotto qualsiasi forma e di riceverne o farne una copia;

(...)

g) di chiedere le registrazioni esistenti relative a conversazioni telefoniche, comunicazioni elettroniche e allo scambio di dati conservate da società di investimento, istituti di credito o istituti finanziari;

h) di chiedere, nella misura in cui ciò sia consentito dal diritto nazionale, le registrazioni esistenti relative allo scambio di dati conservate da un operatore di telecomunicazioni, qualora vi sia il ragionevole sospetto che sia stata commessa una violazione e che tali registrazioni possano essere rilevanti ai fini delle indagini su una violazione dell'articolo 14, lettera a) o b), o dell'articolo 15;

(...)

3. Gli Stati membri provvedono all'adozione di misure appropriate che consentano alle autorità competenti di disporre di tutti i poteri di vigilanza e di indagine necessari allo svolgimento dei loro compiti.

(...)».

### *Diritto francese*

#### *Il CPCE*

20 Il code des postes et des communications électroniques (codice delle poste e delle comunicazioni elettroniche), nella versione applicabile alle controversie principali (in prosieguo: il «CPCE»), all'articolo L. 34-1 così disponeva:

«I. – Il presente articolo si applica al trattamento dei dati personali nell'ambito della fornitura al pubblico di servizi di comunicazione elettronica; in particolare, si applica alle reti che consentono l'operatività dei dispositivi di raccolta di dati e di identificazione.

II. – Gli operatori di comunicazioni elettroniche, e in particolare le persone la cui attività consiste nell'offrire accesso a servizi di comunicazione al pubblico in linea, cancellano o rendono anonimi tutti i dati relativi al traffico, fatte salve le disposizioni dei paragrafi III, IV, V e VI.

Le persone che forniscono al pubblico servizi di comunicazione elettronica predispongono, nel rispetto delle disposizioni del comma precedente, procedure interne che consentano di soddisfare le richieste delle autorità competenti.

Le persone che, nell'esercizio di un'attività professionale principale o accessoria, offrono al pubblico una connessione che consente la comunicazione in linea mediante un accesso alla rete, anche a titolo gratuito, sono tenute al rispetto delle disposizioni applicabili agli operatori di comunicazioni elettroniche in forza del presente articolo.

III. – Ai fini della ricerca, dell'accertamento e del perseguimento dei reati o dell'inadempimento dell'obbligo stabilito dall'articolo L. 336-3 del code de la propriété intellectuelle [codice della proprietà intellettuale] o ai fini della prevenzione degli attacchi ai sistemi di trattamento automatico dei dati previsti e sanzionati dagli articoli da 323-1 a 323-3-1 del code pénal [codice

penale], e al solo scopo di consentire, ove necessario, la messa a disposizione dell'autorità giudiziaria o dell'autorità superiore menzionata all'articolo L. 331-12 del codice della proprietà intellettuale o dell'autorità nazionale per la sicurezza dei sistemi di informazione menzionata all'articolo L. 2321-1 del code de la défense [codice della difesa], possono essere rinviate per un periodo massimo di un anno le operazioni dirette a cancellare o a rendere anonime determinate categorie di dati tecnici. Con decreto adottato a seguito di consultazione del Conseil d'État [Consiglio di Stato], e previo parere della Commission nationale de l'informatique et des libertés [Commissione nazionale per l'informatica e le libertà], sono stabilite, entro i limiti fissati al paragrafo VI, le suddette categorie di dati e la durata della loro conservazione, in funzione dell'attività degli operatori e della natura delle comunicazioni, nonché, se del caso, le modalità di compensazione delle spese identificabili e specifiche delle prestazioni garantite a tale titolo, su richiesta dello Stato, dagli operatori.

(...)

VI. – I dati conservati e trattati alle condizioni di cui ai paragrafi III, IV e V riguardano esclusivamente l'identificazione degli utenti dei servizi prestati dagli operatori, le caratteristiche tecniche delle comunicazioni fornite da questi ultimi e l'ubicazione delle apparecchiature terminali.

Essi non possono riguardare in alcun caso il contenuto della corrispondenza intercorsa o delle informazioni consultate, in qualsiasi forma, nell'ambito di tali comunicazioni.

La conservazione e il trattamento di tali dati sono effettuati nel rispetto delle disposizioni della loi n. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (legge del 6 gennaio 1978, n. 78-17, in materia di informatica, schedari e libertà).

Gli operatori adottano le misure necessarie per impedire l'utilizzo di tali dati a fini diversi da quelli previsti nel presente articolo».

21 L'articolo L. 34-1 del codice delle poste e delle comunicazioni elettroniche, nella versione risultante dalla loi n. 2021-998, du 30 juillet 2021, relative à la prévention d'actes de terrorisme et au renseignement (legge del 30 luglio 2021, n. 2021-998, in materia di prevenzione di atti terroristici e che disciplina i servizi di informazione) (JORF del 31 luglio 2021, testo n. 1), ai paragrafi da II bis a III bis prevede quanto segue:

«II bis. – Gli operatori di comunicazioni elettroniche sono tenuti a conservare:

1° Ai fini dei procedimenti penali, della prevenzione dalle minacce alla pubblica sicurezza e della salvaguardia della sicurezza nazionale, le informazioni relative all'identità anagrafica dell'utente, fino alla scadenza del termine di cinque anni dalla fine della validità del suo contratto;

2° Per gli stessi scopi di cui al punto 1 del presente paragrafo II bis, le altre informazioni fornite dall'utente al momento della sottoscrizione di un contratto o della creazione di un conto nonché le informazioni relative al pagamento, fino alla scadenza del termine di un anno a decorrere dalla fine della validità del suo contratto o dalla chiusura del suo conto;

3° Ai fini della lotta alla criminalità e ai reati gravi, della prevenzione delle minacce gravi alla pubblica sicurezza e della salvaguardia della sicurezza nazionale, i dati tecnici che consentano di identificare la fonte del collegamento o quelli relativi alle apparecchiature terminali impiegate, fino alla scadenza del termine di un anno dal collegamento o dall'impiego delle apparecchiature terminali.

III. – Per ragioni attinenti alla salvaguardia della sicurezza nazionale, qualora venga constatata una minaccia grave, reale o prevedibile, a quest'ultima, il Primo Ministro può, con decreto, ingiungere agli operatori di comunicazioni elettroniche di conservare, per un periodo di un anno, talune categorie di dati relativi al traffico, a integrazione di quelli indicati al punto 3 del paragrafo II bis, e di dati relativi all'ubicazione specificati con decreto adottato a seguito di consultazione del Conseil d'État [Consiglio di Stato].

L'ingiunzione del Primo ministro, la cui durata di applicazione non può superare un anno, può essere rinnovata se continuano a essere soddisfatte le condizioni previste per la sua emanazione. La sua scadenza non incide sul periodo di conservazione dei dati menzionati al primo comma del presente paragrafo III.

III bis. – I dati conservati dagli operatori a norma del presente articolo possono essere oggetto di un'ingiunzione di conservazione rapida da parte delle autorità che dispongono, per legge, dell'accesso ai dati relativi alle comunicazioni elettroniche a fini di prevenzione e repressione della criminalità, dei reati gravi e delle altre gravi violazioni delle norme di cui sono incaricate di garantire il rispetto, al fine di accedere a tali dati».

22 L'articolo R. 10-13 del CPCE è così formulato:

«I. – A norma dell'articolo L. 34-1, paragrafo III, gli operatori di comunicazioni elettroniche conservano, ai fini della ricerca, dell'accertamento e del perseguimento dei reati:

a) le informazioni che consentano di identificare l'utente;

b) i dati relativi alle apparecchiature terminali di comunicazione utilizzate;

c) le caratteristiche tecniche nonché la data, l'ora e la durata di ogni comunicazione;

d) i dati relativi ai servizi complementari richiesti o utilizzati e i loro fornitori;

e) i dati che consentano di identificare il destinatario o i destinatari della comunicazione.

II. – Nel caso delle attività di telefonia, l'operatore conserva i dati di cui al paragrafo II e, inoltre, i dati che consentano di identificare l'origine e l'ubicazione della comunicazione.

III. – I dati di cui al presente articolo sono conservati per un periodo di un anno a decorrere dalla data della loro registrazione.

(...)».

*La LCEN*

23 L'articolo 6 della loi n. 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique (legge del 21 giugno 2004, n. 2004-575, per promuovere la fiducia nell'economia digitale) (JORF del 22 giugno 2004, pag. 11168), nella versione applicabile alle controversie principali (in prosieguo: la «LCEN»), prevedeva quanto segue:

«I. – 1. Le persone la cui attività consiste nell'offrire al pubblico l'accesso a servizi di comunicazione in linea informano i loro abbonati dell'esistenza di mezzi tecnici che consentono di limitare l'accesso a determinati servizi o di selezionarli e propongono loro almeno uno di tali mezzi.

(...)

2. Le persone fisiche o giuridiche che garantiscono, anche a titolo gratuito, mediante la messa a disposizione del pubblico attraverso servizi di comunicazione al pubblico in linea, l'archiviazione di segnali, scritti, immagini, suoni o messaggi di qualsiasi natura forniti dai destinatari di detti servizi non sono civilmente responsabili per le attività o le informazioni archiviate su richiesta di un destinatario di tali servizi se esse non erano effettivamente a conoscenza del loro carattere illecito o di fatti e circostanze da cui risulta tale illiceità o se, dal momento in cui ne hanno avuto conoscenza, hanno agito tempestivamente per ritirare tali dati o renderli inaccessibili.

(...)

II. – Le persone di cui ai punti 1 e 2 del paragrafo I detengono e conservano i dati con modalità tali da permettere l'identificazione di chiunque abbia contribuito alla creazione del contenuto o di uno dei contenuti dei servizi da esse prestati.

Esse forniscono alle persone che pubblicano un servizio di comunicazione al pubblico in linea mezzi tecnici che consentano loro di soddisfare le condizioni di identificazione previste al paragrafo III.

L'autorità giudiziaria può chiedere ai fornitori di cui al paragrafo I, punti 1 e 2, che le siano comunicati i dati indicati nel primo comma.

Al trattamento di tali dati si applicano le disposizioni degli articoli 226-17, 226-21 e 226-22 del codice penale.

Un decreto adottato a seguito di consultazione del Conseil d'État [Consiglio di Stato], e previo parere della Commission nationale de l'informatique et des libertés [Commissione nazionale per l'informatica e le libertà], definisce i dati menzionati nel primo comma e determina la durata e le modalità della loro conservazione.

(...)».

*Il CMF*

24 L'articolo L. 621-10 del code monétaire et financier (codice monetario e finanziario), nella versione applicabile alle controversie principali (in prosieguo: il «CMF»), al primo comma così disponeva:

«Gli inquirenti e gli ispettori possono, a fini d'indagine o di controllo, richiedere tutti i documenti a prescindere dal rispettivo supporto. Gli inquirenti possono anche richiedere i dati conservati e trattati dagli operatori di telecomunicazioni nel quadro dell'articolo L. 34-1 del [CPCE] e dai fornitori menzionati ai punti 1 e 2 del paragrafo I dell'articolo 6 della [LCEN] e ottenerne copia.

(...)».

25 Traendo le conseguenze dalla dichiarazione di illegittimità costituzionale della seconda frase del primo comma dell'articolo L.621-10 del CMF da parte del Conseil constitutionnel (Corte costituzionale, Francia) nella sua decisione del 21 luglio 2017, il legislatore, con la loi n. 2018-898, du 23 octobre 2018, relative à la lutte contre la fraude (legge del 23 ottobre 2018, n. 2018-898, relativa alla lotta alla frode) (JORF del 24 ottobre 2018, testo n. 1), ha inserito nel codice monetario e finanziario l'articolo L. 621-10-2, il quale così recita:

«Ai fini delle indagini sugli abusi di mercato definiti dal regolamento [n. 596/2014], gli inquirenti possono richiedere i dati conservati e trattati dagli operatori di telecomunicazioni, alle condizioni ed entro i limiti previsti all'articolo L. 34-1 del [CPCE], e dai fornitori indicati all'articolo 6, paragrafo I, punti 1 e 2, della [LCEN].

La comunicazione dei dati di cui al primo comma del presente articolo è subordinata all'autorizzazione preventiva di un controllore delle richieste di dati di connessione.

Il controllore delle richieste di dati di connessione è, alternativamente, un membro del Conseil d'État [Consiglio di Stato], in carica od onorario, eletto dall'assemblea generale del Conseil d'État, e un magistrato della Cour de cassation [Corte di cassazione], in carica od onorario, eletto dall'assemblea generale di detta Corte. Il suo supplente, proveniente dall'altro organo giurisdizionale, è designato secondo le stesse modalità. Il controllore delle richieste di dati di connessione e il suo supplente sono eletti per un periodo non rinnovabile di quattro anni.

(...)

Il controllore delle richieste di dati di connessione non può ricevere né richiedere istruzioni dall'Autorità dei mercati finanziari o da altre autorità nell'esercizio delle sue funzioni. Egli è tenuto al segreto professionale alle condizioni previste dall'articolo L. 621-4 del presente codice.

Egli è adito con domanda motivata del segretario generale o del segretario generale aggiunto dell'Autorità dei mercati finanziari. Tale domanda contiene gli elementi atti a giustificarne la fondatezza.

L'autorizzazione è versata al fascicolo d'indagine.

Gli inquirenti utilizzano i dati comunicati dagli operatori di telecomunicazioni e dai fornitori di cui al primo comma del presente articolo esclusivamente nell'ambito dell'indagine per la quale hanno ricevuto l'autorizzazione.

I dati di connessione relativi ai fatti oggetto di notifiche di addebiti da parte del collegio dell'Autorità dei mercati finanziari sono distrutti alla scadenza di un termine di sei mesi a decorrere dalla decisione definitiva della commissione delle sanzioni o degli organi giurisdizionali di ricorso. In caso di composizione amministrativa, il termine di sei mesi decorre dall'esecuzione dell'accordo.

I dati di connessione relativi a fatti che non sono stati oggetto di una notifica di addebiti da parte del collegio dell'Autorità dei mercati finanziari sono distrutti alla scadenza del termine di un mese a decorrere dalla decisione del collegio.

In caso di trasmissione della relazione sull'indagine al procuratore finanziario della Repubblica o in caso di avvio del procedimento penale da parte del procuratore finanziario della Repubblica (...), i dati di connessione sono comunicati al procuratore finanziario della Repubblica e non sono conservati dall'Autorità dei mercati finanziari.

Le modalità di applicazione del presente articolo sono fissate con decreto adottato a seguito di consultazione del Conseil d'État [Consiglio di Stato]».

**Procedimenti principali, questioni pregiudiziali e procedimento dinanzi alla Corte**

26 Con requisitoria introduttiva del 22 maggio 2014 è stata aperta un'istruttoria nei confronti di VD e di SR, vertente su ipotesi di reato qualificate come abuso di informazioni privilegiate e abuso secondario di informazioni privilegiate. Tale istruttoria è stata in seguito estesa, mediante una prima requisitoria integrativa del 14 novembre 2014, al reato di favoreggiamento.

27 Il 23 e il 25 settembre 2015 l'Autorité des marchés financiers (Autorità dei mercati finanziari, Francia) (AMF) ha comunicato al giudice istruttore taluni elementi di cui essa disponeva nell'ambito di un'indagine dalla stessa condotta ai sensi dell'articolo L. 621-10 del CMF, in particolare dati personali provenienti da chiamate telefoniche effettuate da VD e da SR che gli inquirenti dell'AMF avevano raccolto presso operatori di servizi di comunicazione elettronica, sulla base dell'articolo L. 34-1 del CPCE.

28 A seguito della segnalazione così effettuata dall'AMF, l'istruttoria è stata estesa, mediante tre requisitorie integrative del 29 settembre 2015, del 22 dicembre 2015 e del 23 novembre 2016, ai reati di corruzione e riciclaggio.

29 VD e SR sono stati formalmente incriminati, rispettivamente, il 10 marzo e il 29 maggio 2017, per i reati di abuso di informazioni privilegiate e riciclaggio, il primo, e per il reato di abuso di informazioni privilegiate, il secondo.

30 Essendo stati formalmente incriminati sulla base dei dati relativi al traffico forniti dall'AMF, VD e SR hanno proposto ciascuno un ricorso dinanzi alla cour d'appel de Paris (Corte d'appello di Parigi, Francia), deducendo, in particolare, un motivo vertente, in sostanza, sulla violazione dell'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta. In particolare, richiamandosi alla giurisprudenza derivante dalla sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970), VD e SR contestavano il fatto che tale autorità, per procedere alla raccolta di detti dati, si fosse basata sull'articolo L. 621-10 del CMF e sull'articolo L. 34-1 del CPCE, laddove tali disposizioni, da un lato, non sarebbero state conformi al diritto dell'Unione,

in quanto prevedevano una conservazione generalizzata e indiscriminata dei dati di connessione, e, dall'altro, non avrebbero stabilito alcun limite al potere degli inquirenti dell'AMF di richiedere i dati conservati.

31 Con due sentenze della cour d'appel de Paris (Corte d'appello di Parigi) del 20 dicembre 2018 e del 7 marzo 2019, tale giudice ha respinto i ricorsi di VD e di SR. Dalle indicazioni contenute nelle domande di pronuncia pregiudiziale risulta che, per respingere il motivo vertente, in sostanza, sulla violazione dell'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, i giudici di merito si sono basati, in particolare, sul fatto che l'articolo 23, paragrafo 2, lettera h), del regolamento n. 596/2014, relativo agli abusi di mercato, consente alle autorità competenti di chiedere, nella misura in cui ciò sia consentito dal diritto nazionale, le registrazioni esistenti relative allo scambio di dati conservate dagli operatori di servizi di comunicazione elettronica, qualora vi sia il ragionevole sospetto che sia stata commessa una violazione del divieto di abuso di informazioni privilegiate, ai sensi dell'articolo 14, lettere a) e b), di tale regolamento, e che tali registrazioni possano essere rilevanti ai fini delle indagini su tale violazione.

32 VD e SR hanno impugnato tali sentenze dinanzi al giudice del rinvio, deducendo un motivo vertente sulla violazione, in particolare, delle disposizioni della Carta e della direttiva 2002/58 menzionate al punto precedente.

33 Per quanto riguarda l'accesso ai dati di connessione, il giudice del rinvio fa riferimento a una decisione del Conseil constitutionnel (Corte costituzionale) del 21 luglio 2017, da cui risulterebbe che la procedura di accesso ai dati personali conservati dagli inquirenti dell'AMF, quale prevista dal diritto francese, non sarebbe conforme al diritto al rispetto della vita privata, quale tutelato dall'articolo 2 della Déclaration des droits de l'homme et du citoyen de 1789 (Dichiarazione dei diritti dell'uomo e del cittadino del 1789), precisando che, sebbene il legislatore nazionale avesse riservato ad agenti autorizzati e soggetti al rispetto del segreto professionale il potere di ottenere tali dati nell'ambito di un'indagine e non avesse conferito loro un potere di esecuzione forzata, esso non aveva tuttavia corredato detta procedura di alcuna garanzia idonea ad assicurare una conciliazione equilibrata tra, da un lato, il diritto al rispetto della vita privata e, dall'altro, la prevenzione delle minacce all'ordine pubblico e la ricerca degli autori di reati, sicché la seconda frase del primo comma dell'articolo L. 621-10 del CMF doveva essere dichiarata contraria alla Costituzione francese.

34 Il giudice del rinvio rileva inoltre, da un lato, che il Conseil constitutionnel (Corte costituzionale) ha ritenuto che, tenuto conto delle conseguenze «manifestamente eccessive» che un'abrogazione immediata di tale disposizione avrebbe potuto avere sui procedimenti in corso, occorresse differire la data di tale abrogazione al 31 dicembre 2018 e, dall'altro, che il legislatore nazionale, traendo le conseguenze dalla dichiarazione di illegittimità costituzionale del primo comma dell'articolo L. 621-10 del CMF, ha inserito in tale codice l'articolo L. 621-10-2.

35 Il giudice del rinvio, pur ricordando le considerazioni derivanti dal punto 125 della sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970), ritiene che da tale dichiarazione di illegittimità costituzionale non possa risultare la nullità della seconda frase del primo comma dell'articolo L. 621-10 del CMF, applicabile all'epoca dei fatti oggetto dei procedimenti principali, tenuto conto del differimento degli effetti dell'abrogazione di tale disposizione. Esso ritiene tuttavia che la facoltà di cui dispongono gli inquirenti dell'AMF, in

forza di tale disposizione, di ottenere dati di connessione senza previo controllo da parte di un organo giurisdizionale o di un'autorità amministrativa indipendente non sia conforme alle prescrizioni di cui agli articoli 7, 8 e 11 della Carta, quali interpretati dalla Corte.

36 Ciò premesso, si porrebbe al riguardo soltanto la questione della possibilità di rinviare nel tempo gli effetti dell'abrogazione dell'articolo L. 621-10 del CMF, sebbene quest'ultimo non sia conforme alla Carta.

37 Per quanto riguarda la conservazione dei dati di connessione, il giudice del rinvio riferisce anzitutto che, sebbene il paragrafo II dell'articolo L. 34-1 del CPCE sancisca un obbligo di principio, secondo cui gli operatori di servizi di comunicazione elettronica devono cancellare o rendere anonimo qualsiasi dato relativo al traffico, tale obbligo sarebbe tuttavia corredato di una serie di eccezioni, tra cui quella prevista al paragrafo III di tale disposizione, relativa ai «fini della ricerca, dell'accertamento e del perseguimento dei reati». Per tali fini specifici, le operazioni di cancellazione o di anonimizzazione di un determinato numero di dati sarebbero differite di un anno.

38 Esso precisa, al riguardo, che le cinque categorie di dati cui si riferiscono in particolare le condizioni definite al paragrafo III dell'articolo L. 34-1 del CPCE sono quelle elencate all'articolo R. 10-13 del CPCE. Tali dati di connessione sarebbero generati o trattati a seguito di una comunicazione, e sarebbero relativi alle circostanze di tale comunicazione e agli utenti del servizio, ma non fornirebbero alcuna indicazione sul contenuto delle comunicazioni di cui trattasi.

39 Poi, pur richiamando il punto 112 della sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970), secondo cui l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, deve essere interpretato nel senso che esso osta a una normativa nazionale la quale preveda, per finalità di lotta contro la criminalità, una conservazione generalizzata e indiscriminata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica, il giudice del rinvio rileva che, nell'ambito dei procedimenti principali, l'AMF ha avuto accesso ai dati conservati dagli operatori di servizi di comunicazione elettronica in considerazione dei sospetti relativi a un abuso di informazioni privilegiate e ad abusi di mercato potenzialmente integranti vari reati gravi. Tale accesso sarebbe stato giustificato dalla necessità per tale autorità, al fine di garantire l'efficacia della propria indagine, di incrociare diversi dati conservati per un determinato lasso di tempo, per poter aggiornare informazioni privilegiate circolanti tra più interlocutori, che hanno rivelato l'esistenza di pratiche illecite in materia.

40 Secondo il giudice del rinvio, le indagini condotte dall'AMF soddisferebbero gli obblighi posti a carico degli Stati membri dall'articolo 12, paragrafo 2, lettera d), della direttiva 2003/6 e dall'articolo 23, paragrafo 2, lettere g) e h), del regolamento n. 596/2014, letto alla luce dell'articolo 1 del medesimo regolamento, tra cui, in particolare, quello di richiedere la comunicazione delle registrazioni esistenti relative allo scambio di dati conservate dagli operatori di servizi di comunicazione elettronica.

41 Inoltre tale giudice sottolinea, da un lato, richiamando il considerando 65 del regolamento succitato, che tali dati di connessione costituiscono elementi di prova indispensabili, e a volte gli unici elementi di prova disponibili, per individuare e dimostrare l'esistenza di un abuso di

informazioni privilegiate, poiché consentono di determinare l'identità del responsabile della diffusione di informazioni false o fuorvianti, o di stabilire che sono intervenuti contatti tra alcune persone per un certo periodo.

42 Dall'altro lato, il giudice del rinvio cita il considerando 66 del medesimo regolamento, dal quale emerge che l'esercizio dei poteri conferiti alle autorità competenti in materia finanziaria può portare a interferenze con il diritto alla tutela per la vita privata e familiare, il domicilio e le comunicazioni e che, pertanto, gli Stati membri dovrebbero disporre di garanzie adeguate ed efficaci contro ogni abuso, limitando detti poteri ai soli casi in cui sia necessario indagare correttamente su casi gravi in assenza di mezzi equivalenti degli Stati membri per conseguire in modo efficace lo stesso risultato. A suo avviso, da tale considerando risulterebbe che taluni casi di abusi di mercato devono essere considerati come infrazioni gravi.

43 Tale giudice sottolinea, per altro verso, che, nell'ambito dei procedimenti principali, le informazioni privilegiate idonee a qualificare l'elemento materiale quale pratiche illecite in materia di mercato erano, per loro natura, orali e segrete.

44 Alla luce delle considerazioni che precedono, il giudice del rinvio chiede come possa conciliarsi l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, con le prescrizioni di cui all'articolo 12, paragrafo 2, lettera d), della direttiva 2003/6 e all'articolo 23, paragrafo 2, lettere g) e h), del regolamento n. 596/2014.

45 Infine, nel caso in cui la Corte ritenesse che la normativa relativa alla conservazione dei dati di connessione di cui ai procedimenti principali non sia conforme al diritto dell'Unione, si porrebbe la questione del mantenimento provvisorio degli effetti di tale normativa, al fine di evitare un'incertezza del diritto e di consentire che i dati in precedenza raccolti e conservati siano utilizzati ai fini dell'accertamento e del perseguimento dell'abuso di informazioni privilegiate.

46 Ciò considerato, la Cour de cassation (Corte di cassazione) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali, le quali sono formulate in termini identici nelle cause C-339/20 e C-397/20:

«1) Se l'articolo 12, paragrafo 2, lettere a) e d), della direttiva [2003/6] nonché l'articolo 23, paragrafo 2, lettere g) e h), del regolamento [n. 596/2014], che ha sostituito il primo a decorrere dal 3 luglio 2016, letto alla luce del considerando 65 di detto regolamento, non implichino, tenuto conto del carattere occulto delle informazioni scambiate e della generalità del pubblico che può essere coinvolto, la possibilità per il legislatore nazionale di imporre agli operatori di comunicazioni elettroniche una conservazione temporanea ma generalizzata dei dati di connessione, per consentire all'autorità amministrativa di cui [all'articolo] 11 della direttiva [2003/6] e [all'articolo] 22 del regolamento [n. 596/2014], qualora vi siano motivi per sospettare che talune persone siano implicate in un abuso di informazioni privilegiate o in una manipolazione del mercato, di farsi consegnare dall'operatore le registrazioni esistenti relative allo scambio di dati, ove vi sia motivo di sospettare che tali registrazioni connesse all'oggetto dell'indagine possano rivelarsi pertinenti per dimostrare l'esistenza dell'infrazione, in particolare consentendo di risalire ai contatti stretti dagli interessati prima che emergessero i sospetti.

2) Nel caso in cui la risposta della Corte (...) [alla prima questione] fosse tale da indurre la Cour de cassation (Corte di cassazione) a ritenere che la normativa francese sulla conservazione dei dati di connessione non sia conforme al diritto dell'Unione, se gli effetti di tale normativa possano essere mantenuti provvisoriamente al fine di evitare un'incertezza del diritto e di consentire che i dati raccolti e conservati in precedenza siano utilizzati per uno degli scopi previsti da detta normativa.

3) Se un giudice nazionale possa mantenere provvisoriamente gli effetti di una normativa che consente ai funzionari di un'autorità amministrativa indipendente incaricata di svolgere indagini sugli abusi di mercato di ottenere, senza previo controllo da parte di un organo giurisdizionale o di un'altra autorità amministrativa indipendente, la comunicazione dei dati di connessione».

47 Con decisione del presidente della Corte del 17 settembre 2020, le cause C-339/20 e C-397/20 sono state riunite ai fini delle fasi scritta e orale del procedimento nonché della sentenza.

48 Il 21 aprile 2021 il Conseil d'État (Consiglio di Stato, Francia) ha pronunciato la sentenza French Data Network e altri (nn. 393099, 394922, 397844, 397851, 424717, 424718), con la quale esso ha, in particolare, statuito sulla conformità al diritto dell'Unione di talune disposizioni legislative nazionali rilevanti nell'ambito delle controversie principali, ossia l'articolo L. 34-1 del CPCE e l'articolo R. 10-13 del CPCE.

49 Su invito della Corte, i partecipanti all'udienza nelle presenti cause hanno avuto l'opportunità di pronunciarsi sull'eventuale incidenza, per i rinvii pregiudiziali in esame, di tale sentenza del Conseil d'État (Consiglio di Stato).

50 Il rappresentante del governo francese ha affermato, in occasione di tale udienza, che, con detta sentenza, il Conseil d'État (Consiglio di Stato) ha, in sostanza, dichiarato illegittime le disposizioni che consentono di attuare la conservazione generalizzata e indiscriminata dei dati di connessione a fini di lotta alla criminalità, ad eccezione della conservazione degli indirizzi IP e dei dati relativi all'identità anagrafica degli utenti delle reti di comunicazione elettronica, traendo così le conseguenze dalla 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). Esso ha tuttavia precisato che, in sede contenziosa, il Conseil d'État (Consiglio di Stato) doveva anche rispondere all'obiezione del governo francese secondo la quale tale interpretazione del diritto dell'Unione contrasterebbe con norme di rango costituzionale, vale a dire quelle riguardanti la prevenzione delle minacce all'ordine pubblico, in particolare alla sicurezza delle persone e dei beni, e la ricerca degli autori di reati.

51 Al riguardo, il rappresentante del governo francese ha spiegato che il Conseil d'État (Consiglio di Stato) aveva respinto tale obiezione in due fasi. Da un lato, esso avrebbe indubbiamente riconosciuto che la conservazione generalizzata e indiscriminata dei dati di connessione era una condizione determinante del successo delle indagini penali e che nessun altro metodo poteva utilmente sostituirvisi. Dall'altro lato, nondimeno, il Conseil d'État (Consiglio di Stato) avrebbe ritenuto, fondandosi, in particolare, sul punto 164 della 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), che la conservazione rapida dei dati sarebbe autorizzata dal diritto dell'Unione anche laddove tale conservazione rapida vertesse su dati inizialmente conservati a fini di salvaguardia della sicurezza nazionale.

52 Inoltre, il rappresentante del governo francese ha precisato che, a seguito della sentenza del Conseil d'État (Consiglio di Stato), del 21 aprile 2021, French Data Network e altri (nn. 393099, 394922, 397844, 397851, 424717, 424718), il legislatore nazionale avrebbe inserito il paragrafo III bis all'articolo L. 34-1 del codice delle poste e delle comunicazioni elettroniche, quale menzionato al punto 21 della presente sentenza.

## Sulle questioni pregiudiziali

### *Osservazioni preliminari*

53 In primo luogo, occorre ricordare che, successivamente alla presentazione delle domande di pronuncia pregiudiziale in esame, il Conseil d'État (Consiglio di Stato) ha pronunciato la sentenza del 21 aprile 2021, French Data Network e altri (nn. 393099, 394922, 397844, 397851, 424717, 424718), vertente, in particolare, sulla conformità al diritto dell'Unione dell'articolo L. 34 -1 del CPCE e dell'articolo R. 10-13 del CPCE.

54 Orbene, come rilevato dall'avvocato generale al paragrafo 42 delle sue conclusioni, e come risulta altresì dalle spiegazioni fornite dal giudice del rinvio, quali esposte ai punti 27, 37 e 38 della presente sentenza, tali articoli costituiscono «disposizioni chiave» nell'ambito dell'applicazione dell'articolo L. 621-10 del CMF, che è in discussione nei procedimenti principali.

55 All'udienza dinanzi alla Corte, il rappresentante del governo francese, dopo aver posto l'accento sull'evoluzione legislativa di cui è stato oggetto l'articolo L. 34-1 del CPCE a seguito delle precisazioni fornite dalla Corte nella 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), quale menzionata al punto 21 della presente sentenza, ha affermato, in sostanza, che, per risolvere le controversie di cui ai procedimenti principali, il giudice del rinvio sarebbe indotto, conformemente al principio di applicazione della legge nel tempo sancito agli articoli 7 e 8 della Dichiarazione dei diritti dell'uomo e del cittadino del 1789, a tener conto delle disposizioni nazionali nella versione applicabile ai fatti oggetto dei procedimenti principali, i quali risalgono agli anni 2014 e 2015, sicché la sentenza del Conseil d'État (Consiglio di Stato) del 21 aprile 2021, French Data Network e altri (nn. 393099, 394922, 397844, 397851, 424717, 424718), non potrebbe, in ogni caso, essere presa in considerazione ai fini dell'analisi delle domande di pronuncia pregiudiziale in esame.

56 Secondo una costante giurisprudenza, nell'ambito del procedimento istituito dall'articolo 267 TFUE, spetta esclusivamente al giudice nazionale, cui è stata sottoposta la controversia e che deve assumersi la responsabilità dell'emananda decisione giurisdizionale, valutare, alla luce delle particolari circostanze della causa, sia la necessità di una pronuncia pregiudiziale per essere in grado di pronunciare la propria sentenza sia la rilevanza delle questioni che sottopone alla Corte. Di conseguenza, se le questioni sollevate vertono sull'interpretazione del diritto dell'Unione, la Corte, in via di principio, è tenuta a pronunciarsi (v., in tal senso, sentenza dell'8 settembre 2010, Winner Wetten, C-409/06, EU:C:2010:503, punto 36 e giurisprudenza ivi citata).

57 La Corte può rifiutare di pronunciarsi su una questione pregiudiziale sollevata da un giudice nazionale solo qualora risulti manifestamente che l'interpretazione del diritto dell'Unione richiesta non ha alcun rapporto con la realtà effettiva o con l'oggetto della controversia principale, qualora il problema sia di natura teorica oppure nel caso in cui la Corte non disponga

degli elementi di fatto e di diritto necessari per fornire una risposta utile alle questioni che le vengono sottoposte (v., in tal senso, sentenza del 19 novembre 2009, Filipiak, C-314/08, EU:C:2009:719, punto 42 e giurisprudenza ivi citata).

58 Nel caso di specie, dalle decisioni di rinvio risulta che le questioni pregiudiziali prima e terza riguardano direttamente non già l'articolo L. 34-1 del CPCE e l'articolo R. 10-13 del CPCE, bensì l'articolo L. 621-10 del CMF, in forza del quale l'AMF ha chiesto agli operatori di servizi di comunicazione elettronica la comunicazione dei dati relativi al traffico riguardanti chiamate telefoniche effettuate da VD e da SR, sulla base dei quali questi ultimi sono stati formalmente incriminati e la cui ammissibilità come elementi di prova è contestata nell'ambito dei procedimenti principali.

59 Inoltre occorre rilevare che, con le questioni pregiudiziali seconda e terza sollevate nelle presenti cause, che si inseriscono nel solco della prima questione, il giudice del rinvio chiede in sostanza se, nell'ipotesi in cui la normativa nazionale di cui trattasi, relativa alla conservazione e all'accesso dei dati di connessione, dovesse rivelarsi non conforme al diritto dell'Unione, i suoi effetti non possano tuttavia essere provvisoriamente mantenuti, in modo da evitare un'incertezza del diritto e da consentire che i dati conservati sulla base di tale normativa possano essere utilizzati ai fini dell'accertamento e del perseguimento dell'abuso di informazioni privilegiate.

60 Alla luce degli elementi che precedono, nonché di quelli rilevati dall'avvocato generale ai paragrafi da 44 a 47 delle sue conclusioni, si deve giudicare che, indipendentemente dalla sentenza del Conseil d'État (Consiglio di Stato) del 21 aprile 2021, French Data Network e altri (nn. 393099, 394922, 397844, 397851, 424717, 424718), nonché dalla decisione del Conseil constitutionnel (Corte costituzionale) del 25 febbraio 2022 (n. 2021-976/977), che ha dichiarato incostituzionale in parte l'articolo L. 34-1 del CPCE, nella versione riportata al punto 20 della presente sentenza, una risposta della Corte alle questioni sollevate rimane necessaria per la soluzione delle controversie di cui ai procedimenti principali.

61 In secondo luogo, occorre rilevare che, all'udienza dinanzi alla Corte, il rappresentante di VD ha contestato l'applicabilità ratione temporis del regolamento n. 596/2014 affermando, in sostanza, che i fatti oggetto dei procedimenti principali si sarebbero verificati prima dell'entrata in vigore di tale regolamento. Pertanto, solo le disposizioni della direttiva 2003/6 sarebbero rilevanti ai fini dell'esame delle questioni pregiudiziali sollevate dal giudice del rinvio.

62 A tale riguardo va ricordato che, secondo una giurisprudenza costante, una nuova norma giuridica si applica a decorrere dall'entrata in vigore dell'atto che l'istituisce e, sebbene non si applichi alle situazioni giuridiche sorte e definitivamente consolidatesi in vigenza della vecchia legge, si applica agli effetti futuri delle medesime, nonché alle situazioni giuridiche nuove, salvo il caso in cui, fatto salvo il principio di irretroattività degli atti giuridici, la nuova norma sia accompagnata da disposizioni particolari che determinino specificamente le sue condizioni di applicazione nel tempo (v., in tal senso, sentenze del 15 gennaio 2019, E.B., C-258/17, EU:C:2019:17, punto 50 e giurisprudenza ivi citata, e del 14 maggio 2020, Azienda Municipale Ambiente, C-15/19, EU:C:2020:371, punto 57).

63 Orbene, come rilevato ai punti da 26 a 29 della presente sentenza, sebbene le situazioni giuridiche oggetto dei procedimenti principali siano effettivamente sorte prima dell'entrata in vigore del regolamento n. 596/2014, il quale ha abrogato e sostituito la direttiva 2003/6 con effetto dal

3 luglio 2016, i procedimenti principali hanno seguito il loro corso dopo tale data cosicché, a decorrere da quest'ultima, gli effetti futuri di tali situazioni sono, conformemente al principio ricordato al punto precedente, disciplinati dal regolamento n. 596/2014.

64 Ne consegue che le disposizioni del regolamento n. 596/2014 sono applicabili al caso di specie. Per altro verso, non si devono operare distinzioni tra le disposizioni richiamate dal giudice del rinvio risultanti dalla direttiva 2003/6 e quelle risultanti dal regolamento n. 596/2014, in quanto queste ultime hanno una portata sostanzialmente simile ai fini dell'interpretazione che la Corte sarà chiamata a fornire nell'ambito delle presenti cause.

### *Sulla prima questione*

65 Con la prima questione pregiudiziale il giudice del rinvio chiede, in sostanza, se l'articolo 12, paragrafo 2, lettere a) e d), della direttiva 2003/6 e l'articolo 23, paragrafo 2, lettere g) e h), del regolamento n. 596/2014, in combinato disposto con l'articolo 15, paragrafo 1, della direttiva 2002/58, e alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, debbano essere interpretati nel senso che essi ostano a misure legislative come quella oggetto dei procedimenti principali che prevedono, a titolo preventivo, per finalità di contrasto dei reati di abuso di mercato, di cui fa parte l'abuso di informazioni privilegiate, una conservazione generalizzata e indiscriminata dei dati relativi al traffico per un anno a decorrere dal giorno della registrazione.

66 Le parti nel procedimento principale e gli interessati che hanno presentato osservazioni scritte alla Corte hanno espresso pareri divergenti al riguardo. Secondo il governo estone, l'Irlanda e i governi spagnolo e francese, l'articolo 12, paragrafo 2, lettere a) e d), della direttiva 2003/6 e l'articolo 23, paragrafo 2, lettere g) e h), del regolamento n. 596/2014 autorizzano implicitamente, ma necessariamente, il legislatore nazionale a imporre, in capo agli operatori di servizi di comunicazione elettronica, un obbligo di conservazione generalizzata e indiscriminata dei dati, al fine di consentire all'autorità competente in materia finanziaria di individuare e sanzionare gli abusi di informazioni privilegiate. Giacché, come risulta dal considerando 65 del regolamento n. 596/2014, dette registrazioni costituiscono elementi di prova indispensabili, e a volte gli unici elementi di prova disponibili, per individuare e dimostrare l'esistenza dell'abuso di informazioni privilegiate, un simile obbligo di conservazione sarebbe indispensabile sia per garantire l'efficacia delle indagini e delle azioni giudiziarie compiute da detta autorità, e con ciò l'efficacia pratica dell'articolo 12, paragrafo 2, lettere a) e d), della direttiva 2003/6 nonché dell'articolo 23, paragrafo 2, lettera h), del regolamento n. 596/2014, sia per rispondere agli obiettivi di interesse generale perseguiti da tali strumenti, volti a garantire l'integrità dei mercati finanziari dell'Unione e a rafforzare la fiducia degli investitori in tali mercati.

67 VD, SR, il governo polacco e la Commissione europea sostengono invece che le disposizioni succitate, in quanto si limitano a circoscrivere il potere di richiedere, agli operatori di servizi di comunicazione elettronica, la comunicazione delle registrazioni «esistenti» relative allo scambio di dati conservate da tali operatori, disciplinano soltanto la questione dell'accesso a tali dati.

68 A tale riguardo, va ricordato in primo luogo che, secondo una giurisprudenza costante, ai fini dell'interpretazione di una norma del diritto dell'Unione non si deve soltanto fare riferimento al tenore letterale della stessa, ma anche tenere conto del suo contesto e degli scopi perseguiti dalla normativa di cui essa fa parte e prendere in considerazione, in particolare, la genesi di tale normativa (v., in tal senso, sentenza del 17 aprile 2018, Egenberger, C-414/16, EU:C:2018:257, punto 44).

69 Per quanto concerne il tenore letterale delle disposizioni menzionate nella prima questione pregiudiziale occorre constatare che, mentre l'articolo 12, paragrafo 2, lettera d), della direttiva 2003/6 fa riferimento al potere dell'autorità competente in materia finanziaria di «richiedere le registrazioni telefoniche esistenti e le informazioni esistenti relative al traffico», l'articolo 23, paragrafo 2, lettere g) e h), del regolamento n. 596/2014 rinvia al potere di tale autorità di chiedere, da un lato, le «registrazioni esistenti relative (...) allo scambio di dati conservate da società di investimento, istituti di credito o istituti finanziari» e, dall'altro, «nella misura in cui ciò sia consentito dal diritto nazionale, le registrazioni esistenti relative allo scambio di dati conservate da un operatore di telecomunicazioni».

70 Orbene, dal tenore letterale di tali disposizioni emerge inequivocabilmente che esse si limitano a circoscrivere il potere della suddetta autorità di «richiedere» o, ancora, di «chiedere» i dati di cui tali operatori dispongono, il che corrisponde a un accesso a tali dati. Inoltre, il riferimento alle registrazioni «esistenti», quali «conservate» da detti operatori, lascia intendere che il legislatore dell'Unione non ha inteso disciplinare la possibilità, per il legislatore nazionale, di introdurre un obbligo di conservazione di simili registrazioni.

71 A tale riguardo è opportuno ricordare che, secondo una giurisprudenza costante, l'interpretazione di una disposizione del diritto dell'Unione non può avere come risultato di privare di ogni efficacia pratica la formulazione chiara e precisa di tale disposizione. Pertanto, allorché il senso di una disposizione del diritto dell'Unione risulta senza ambiguità dalla formulazione stessa di quest'ultima, la Corte non può discostarsi da tale interpretazione (sentenza del 25 gennaio 2022, VYSOČINA WIND, C-181/20, EU:C:2022:51, punto 39 e giurisprudenza ivi citata).

72 L'interpretazione delineata al punto 70 della presente sentenza è avvalorata sia dal contesto in cui si inseriscono l'articolo 12, paragrafo 2, lettere a) e d), della direttiva 2003/6 e l'articolo 23, paragrafo 2, lettere g) e h), del regolamento n. 596/2014 sia dagli obiettivi perseguiti dalla normativa di cui tali disposizioni fanno parte.

73 Per quanto riguarda il contesto in cui si inseriscono tali disposizioni occorre osservare che, sebbene, ai sensi dell'articolo 12, paragrafo 1, della direttiva 2003/6 e dell'articolo 23, paragrafo 3, del regolamento n. 596/2014, letto alla luce del considerando 62 del medesimo regolamento, il legislatore dell'Unione abbia inteso imporre agli Stati membri di adottare le misure necessarie affinché le autorità competenti in materia finanziaria dispongano di una serie di strumenti, poteri e risorse adeguati, nonché dei poteri di vigilanza e indagine necessari per garantire l'efficacia dei loro compiti, tali disposizioni nulla dicono né sull'eventuale possibilità per gli Stati membri di imporre, a tali fini, a carico degli operatori di servizi di comunicazione elettronica, un obbligo di conservazione generalizzata e indiscriminata dei dati relativi al traffico né sulle condizioni alle quali tali dati devono essere conservati dagli stessi operatori ai fini della loro eventuale consegna alle autorità competenti.

74 Con l'articolo 12, paragrafo 2, della direttiva 2003/6 e l'articolo 23, paragrafo 2, del regolamento n. 596/2014, il legislatore dell'Unione ha unicamente inteso investire l'autorità competente in materia finanziaria, al fine di garantire l'efficacia dei suoi compiti di indagine e vigilanza, di classici poteri investigativi, come quelli che consentono a tale autorità di accedere a documenti, di eseguire ispezioni e perquisizioni, o ancora di pronunciare ingiunzioni o divieti nei confronti di persone sospettate di aver commesso reati di abuso di mercato, di cui fa parte, in particolare, l'abuso di informazioni privilegiate.

75 Per altro verso, è necessario constatare che le disposizioni del regolamento n. 596/2014 che disciplinano specificamente la questione della conservazione dei dati, ossia l'articolo 11, paragrafo 5, ultimo comma, paragrafo 6, secondo comma, paragrafo 8 e paragrafo 11, lettera c), l'articolo 17, paragrafo 1, primo comma, l'articolo 18, paragrafo 5, e l'articolo 28 di tale regolamento, prevedono un simile obbligo di conservazione solo in capo agli operatori finanziari, quali elencati all'articolo 23, paragrafo 2, lettera g), dello stesso regolamento, e riguardano, pertanto, unicamente i dati relativi a operazioni finanziarie e a servizi forniti da tali operatori specifici.

76 Per quanto riguarda gli obiettivi perseguiti dalla normativa di cui trattasi, occorre osservare che dai considerando 2 e 12 della direttiva 2003/6, da un lato, e dall'articolo 1 del regolamento n. 596/2014, letto alla luce dei considerando 2 e 24 del medesimo, dall'altro, risulta che tali strumenti hanno lo scopo di garantire l'integrità dei mercati finanziari dell'Unione e di rafforzare la fiducia degli investitori in tali mercati, fiducia che poggia, in particolare, sul fatto che essi saranno posti su un piano di parità e tutelati dall'abuso di informazioni privilegiate. Il divieto dell'abuso di informazioni privilegiate stabilito all'articolo 2, paragrafo 1, della direttiva 2003/6 e all'articolo 8, paragrafo 1, del regolamento n. 596/2014 è volto pertanto a garantire la parità dei partecipanti a una compravendita di borsa evitando che uno di loro, che detenga un'informazione privilegiata e si trovi, perciò, in una posizione avvantaggiata rispetto agli altri investitori, ne tragga profitto a scapito di coloro che la ignorano (v., in tal senso, sentenza del 15 marzo 2022, Autorité des marchés financiers, C-302/20, EU:C:2022:190, punti 43, 65 e 77 e giurisprudenza ivi citata).

77 Se è vero che, ai sensi del considerando 65 del regolamento n. 596/2014, le registrazioni dei dati di connessione costituiscono elementi di prova indispensabili, e a volte gli unici che consentono di individuare e dimostrare l'esistenza dell'abuso di informazioni privilegiate e di manipolazione del mercato, resta il fatto che tale considerando si riferisce soltanto alle registrazioni «detenute» dagli operatori di servizi di comunicazione elettronica nonché al potere dell'autorità competente in materia finanziaria di «richiedere», presso tali operatori, la comunicazione dei dati «esistenti». Pertanto, da tale considerando non risulta affatto che il legislatore dell'Unione, con tale regolamento, abbia inteso riconoscere agli Stati membri il potere di imporre agli operatori di servizi di comunicazione elettronica un obbligo generale di conservazione dei dati.

78 Alla luce degli elementi che precedono, si deve ritenere che né la direttiva 2003/6 né il regolamento n. 596/2014 possano essere interpretati nel senso che possono costituire il fondamento giuridico di un obbligo generale di conservazione delle registrazioni di dati relativi al traffico, detenuti dagli operatori di servizi di comunicazione elettronica ai fini dell'esercizio dei poteri conferiti all'autorità competente in materia finanziaria in forza della direttiva 2003/6 e del regolamento n. 596/2014.

79 In secondo luogo, occorre ricordare che, come rilevato in sostanza dall'avvocato generale ai paragrafi 53 e 61 delle sue conclusioni, la direttiva 2002/58 costituisce l'atto di riferimento in materia di conservazione e, più in generale, di trattamento dei dati personali nel settore delle comunicazioni elettroniche, cosicché l'interpretazione data dalla Corte alla luce di tale direttiva vale anche per le registrazioni dei dati relativi al traffico detenute dagli operatori di servizi di comunicazione elettronica, che le autorità competenti in materia finanziaria, ai sensi dell'articolo 11 della direttiva 2003/6 e dell'articolo 22 del regolamento n. 596/2014, possono richiedere loro.

80 Ai sensi dell'articolo 1, paragrafo 1, della direttiva 2002/58, infatti, essa prevede, in particolare, l'armonizzazione delle disposizioni nazionali necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata e alla riservatezza, riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche, il quale ultimo comprende anche il settore delle telecomunicazioni.

81 Per altro verso, dall'articolo 3 di tale direttiva risulta che essa si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche nell'Unione, comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e identificazione dei dati. Pertanto, la citata direttiva deve essere considerata come disciplinante le attività dei fornitori di tali servizi, tra i quali figurano, in particolare, gli operatori di telecomunicazioni (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, punto 93 e giurisprudenza ivi citata).

82 Tenuto conto degli elementi che precedono, si deve ritenere che, come rilevato in sostanza dall'avvocato generale ai paragrafi 62 e 63 delle sue conclusioni, la valutazione della liceità del trattamento delle registrazioni conservate dagli operatori di servizi di comunicazione elettronica, ai sensi dell'articolo 12, paragrafo 2, lettera d), della direttiva 2003/6 e dell'articolo 23, paragrafo 2, lettere g) e h), del regolamento n. 596/2014, debba essere effettuata alla luce delle condizioni previste dalla direttiva 2002/58, nonché dell'interpretazione di tale direttiva nella giurisprudenza della Corte.

83 Tale interpretazione è corroborata dall'articolo 3, paragrafo 1, punto 27, del regolamento n. 596/2014, il quale prevede che le registrazioni di dati relativi al traffico ai fini di tale regolamento sono quelle definite all'articolo 2, secondo comma, lettera b), della direttiva 2002/58.

84 Inoltre, ai sensi del considerando 44 della direttiva 2003/6, nonché dei considerando 66 e 77 del regolamento n. 596/2014, le finalità contemplate da tali atti devono essere perseguite nel rispetto dei diritti fondamentali e dei principi sanciti dalla Carta, compreso il diritto alla tutela della vita privata. A tale riguardo, il legislatore dell'Unione ha espressamente precisato, al considerando 66 del regolamento n. 596/2014, che, per esercitare i poteri conferiti all'autorità competente in materia finanziaria, in forza di tale regolamento, che possono portare a gravi interferenze con il diritto alla tutela per la vita privata e familiare, il domicilio e le comunicazioni, gli Stati membri dovrebbero disporre di garanzie adeguate ed efficaci contro ogni abuso, come ad esempio un requisito per ottenere, se necessario, un'autorizzazione preventiva da parte delle autorità giudiziarie dello Stato membro interessato. Gli Stati membri dovrebbero prevedere la possibilità che le autorità competenti esercitino tali poteri invasivi nella misura necessaria per indagare correttamente su casi gravi, in assenza di mezzi equivalenti per conseguire in modo efficace lo stesso risultato. Ne consegue che l'applicazione delle misure disciplinate dalla direttiva 2003/6 e dal regolamento n. 596/2014 non può, in ogni caso, pregiudicare la protezione dei dati personali conferita ai sensi della direttiva 2002/58 (v. in tal senso, per analogia, sentenze del 29 gennaio 2008, Promusicae, C-275/06, EU:C:2008:54, punto 57, e del 17 giugno 2021, M.I.C.M., C-597/19, EU:C:2021:492, punto 124 e giurisprudenza ivi citata).

85 Di conseguenza, l'articolo 12, paragrafo 2, lettere a) e d), della direttiva 2003/6 e l'articolo 23, paragrafo 2, lettere g) e h), del regolamento n. 596/2014 devono essere interpretati nel senso che essi non autorizzano una conservazione generalizzata e indiscriminata dei dati relativi al traffico e dei dati relativi all'ubicazione per finalità di contrasto di reati di abuso di mercato e, in particolare, di abuso di informazioni privilegiate, fermo restando che la compatibilità con il

diritto dell'Unione di una normativa nazionale che prevede una simile conservazione deve essere valutata in rapporto all'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, quale interpretato dalla giurisprudenza della Corte.

86 Per quanto attiene all'esame della compatibilità di una tale normativa nazionale con queste ultime disposizioni va ricordato che, come risulta in sostanza da una lettura combinata dei punti 53, 54 e 58 della presente sentenza, se è vero che la disposizione al centro dei rinvii pregiudiziali in esame è l'articolo L. 621-10 del CMF, ai sensi del quale l'AMF ha chiesto agli operatori di servizi di comunicazione elettronica la trasmissione dei dati relativi al traffico riguardanti chiamate telefoniche effettuate da VD e SR, sulla base dei quali questi ultimi sono stati formalmente incriminati, ciò non toglie che, come rilevato dall'avvocato generale al paragrafo 42 delle sue conclusioni, l'articolo L. 34-1 del CPCE et l'articolo R. 10-13 del CPCE costituiscono «disposizioni chiave» nell'ambito dell'applicazione di tale articolo L. 621-10 del CMF.

87 Invero, dalle spiegazioni fornite dal giudice del rinvio, come sintetizzate ai punti 27, 37 e 38 della presente sentenza, risulta che, da un lato, gli inquirenti dell'AMF avevano raccolto i dati relativi al traffico di cui trattasi sulla base dell'articolo L. 34-1 del CPCE, nella versione applicabile alle controversie principali, il cui paragrafo III corredava l'obbligo di principio previsto al paragrafo II, secondo il quale gli operatori di servizi di comunicazione elettronica dovevano cancellare o rendere anonimo qualsiasi dato relativo al traffico, di una serie di eccezioni, compresa quella relativa ai «fini della ricerca, dell'accertamento e del perseguimento dei reati». Per tali fini specifici, le operazioni di cancellazione o di anonimizzazione di un determinato numero di dati erano differite di un anno.

88 Dall'altro lato, tale giudice precisa che le cinque categorie di dati di cui al paragrafo III dell'articolo L. 34-1 del CPCE, nella versione applicabile alle controversie principali, erano quelle elencate all'articolo R. 10-13 del CPCE, ossia le informazioni che consentivano di identificare l'utente, i dati relativi alle apparecchiature terminali di comunicazione utilizzate, le caratteristiche tecniche, la data, l'ora e la durata di ciascuna comunicazione, i dati relativi ai servizi complementari richiesti o utilizzati e i loro fornitori e, infine, i dati che consentivano di identificare il destinatario o i destinatari della comunicazione. Dal paragrafo II dell'articolo R. 10-13 del CPCE, nella versione applicabile alle controversie principali, risulta inoltre che, per le attività di telefonia, gli operatori interessati potevano anche conservare i dati che consentivano di individuare l'origine e l'ubicazione della comunicazione.

89 Ne consegue che la normativa di cui ai procedimenti principali interessa l'insieme dei mezzi di comunicazione elettronica e comprende tutti gli utenti di tali mezzi, senza che sia operata al riguardo alcuna distinzione o eccezione. Inoltre, i dati che tale normativa impone agli operatori di servizi di comunicazione elettronica di conservare sono, in particolare, quelli necessari per individuare l'origine e la destinazione di una comunicazione, determinare la data, l'ora, la durata e il tipo di comunicazione, identificare lo strumento di comunicazione utilizzato nonché localizzare le apparecchiature terminali e le comunicazioni, dati tra i quali figurano, in particolare, il nome e l'indirizzo dell'utente nonché i numeri di telefono del chiamante e del chiamato.

90 Pertanto, i dati che, in forza della normativa nazionale in questione, devono essere conservati per un anno, benché non comprendano il contenuto delle comunicazioni di cui trattasi, consentono, in particolare, di sapere chi sia la persona con cui ha comunicato l'utente di un mezzo di comunicazione telefonica e con quale mezzo sia stata effettuata tale comunicazione, di

determinare la data, l'ora e la durata delle comunicazioni nonché il luogo a partire dal quale esse sono state effettuate, e di conoscere l'ubicazione delle apparecchiature terminali senza che sia necessariamente effettuata una comunicazione. Inoltre, essi consentono di determinare la frequenza delle comunicazioni dell'utente con talune persone durante un periodo determinato. Pertanto si deve ritenere che tali dati, presi nel loro insieme, siano idonei a consentire di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini della vita quotidiana, i luoghi di soggiorno permanenti o temporanei, gli spostamenti giornalieri o di altro tipo, le attività esercitate, le relazioni sociali di dette persone e gli ambienti sociali da esse frequentati. In particolare, questi dati forniscono gli strumenti per stabilire il profilo degli interessati, informazione tanto delicata, in rapporto al diritto al rispetto della vita privata, quanto il contenuto stesso delle comunicazioni (v., in tal senso, sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 45 e giurisprudenza ivi citata).

91 Quanto alle finalità perseguite, occorre rilevare che la normativa in questione riguarda, tra le altre finalità, la ricerca, l'accertamento e il perseguimento dei reati, ivi compresi quelli relativi agli abusi di mercato di cui fa parte l'abuso di informazioni privilegiate.

92 Tenuto conto degli elementi esposti ai punti da 86 a 91 della presente sentenza, si deve constatare che, con la normativa di cui trattasi, il legislatore nazionale ha previsto, ai fini, in particolare, della ricerca, dell'accertamento e del perseguimento dei reati e del contrasto alla criminalità, una conservazione generalizzata e indiscriminata dei dati relativi al traffico per un anno a decorrere dal giorno della registrazione.

93 Orbene, dai punti da 140 a 168 della 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), nonché dai punti da 59 a 101 della sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a. (C-140/20, EU:C:2022:258), risulta in particolare che una simile conservazione non può essere giustificata da obiettivi del genere in forza dell'articolo 15, paragrafo 1, della direttiva 2002/58.

94 Ne consegue che una normativa nazionale, come quella di cui ai procedimenti principali, che impone agli operatori di servizi di comunicazione elettronica di procedere, a titolo preventivo, per finalità di contrasto dei reati di abuso di mercato, di cui fa parte l'abuso di informazioni privilegiate, a una conservazione generalizzata e indiscriminata dei dati relativi al traffico di tutti gli utenti dei mezzi di comunicazione elettronica, senza che sia operata alcuna distinzione al riguardo o che siano previste eccezioni e senza che il rapporto richiesto, ai sensi della giurisprudenza menzionata al punto precedente, tra i dati da conservare e l'obiettivo perseguito sia dimostrato, eccede i limiti dello stretto necessario e non può essere considerata giustificata, in una società democratica, come richiede l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta (v., in tal senso, per analogia, sentenza del 6 ottobre 2020, Privacy International, C-623/17, EU:C:2020:790, punto 81).

95 Alla luce degli elementi che precedono, occorre rispondere alla prima questione pregiudiziale nelle cause C-339/20 e C-397/20 dichiarando che l'articolo 12, paragrafo 2, lettere a) e d), della direttiva 2003/6 e l'articolo 23, paragrafo 2, lettere g) e h), del regolamento n. 596/2014, in combinato disposto con l'articolo 15, paragrafo 1, della direttiva 2002/58, e alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, devono essere interpretati nel senso che essi ostano a misure legislative che prevedono, a titolo preventivo, per finalità di

contrasto dei reati di abuso di mercato, di cui fa parte l'abuso di informazioni privilegiate, una conservazione generalizzata e indiscriminata dei dati relativi al traffico per un anno a decorrere dal giorno della registrazione.

***Sulle questioni seconda e terza***

96 Con le questioni pregiudiziali seconda e terza nelle presenti cause, che è opportuno esaminare congiuntamente, il giudice del rinvio chiede, in sostanza, se il diritto dell'Unione debba essere interpretato nel senso che un giudice nazionale può limitare nel tempo gli effetti di una declaratoria di invalidità, in forza del diritto nazionale, nei confronti delle disposizioni legislative nazionali che, da un lato, impongono agli operatori di servizi di comunicazione elettronica una conservazione generalizzata e indiscriminata dei dati relativi al traffico e, dall'altro, consentono la comunicazione di simili dati all'autorità competente in materia finanziaria, senza previa autorizzazione di un organo giurisdizionale o di un'autorità amministrativa indipendente, a causa dell'incompatibilità di tale normativa con l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce della Carta.

97 Occorre senz'altro ricordare che il principio del primato del diritto dell'Unione sancisce la preminenza del diritto dell'Unione sul diritto degli Stati membri. Tale principio impone pertanto a tutte le istituzioni degli Stati membri di dare pieno effetto alle varie disposizioni del diritto dell'Unione, dato che il diritto degli Stati membri non può sminuire l'efficacia riconosciuta a tali disposizioni nel territorio dei suddetti Stati. In forza di tale principio, ove non sia possibile procedere a un'interpretazione della normativa nazionale conforme alle prescrizioni del diritto dell'Unione, il giudice nazionale incaricato di applicare, nell'ambito di propria competenza, le disposizioni di diritto dell'Unione ha l'obbligo di garantire la piena efficacia delle medesime, disapplicando all'occorrenza, di propria iniziativa, qualsiasi disposizione contrastante della legislazione nazionale, anche posteriore, senza doverne chiedere o attendere la previa rimozione in via legislativa o mediante qualsiasi altro procedimento costituzionale (v., in tal senso, sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 118 e giurisprudenza ivi citata).

98 Solo la Corte può, eccezionalmente e per considerazioni imperative di certezza del diritto, concedere una sospensione provvisoria dell'effetto di disapplicazione esercitato da una norma di diritto dell'Unione rispetto a norme di diritto interno con essa in contrasto. Una siffatta limitazione nel tempo degli effetti dell'interpretazione data dalla Corte a tale diritto può essere concessa solo nella stessa sentenza che statuisce sull'interpretazione richiesta. Il primato e l'applicazione uniforme del diritto dell'Unione risulterebbero pregiudicati se i giudici nazionali avessero il potere di attribuire alle norme nazionali, anche solo provvisoriamente, il primato rispetto al diritto dell'Unione al quale esse contravvengono (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 119 e giurisprudenza ivi citata).

99 Vero è che la Corte ha giudicato, in una causa riguardante la legittimità di misure adottate in violazione dell'obbligo sancito dal diritto dell'Unione di effettuare una valutazione preliminare dell'impatto di un progetto sull'ambiente e su un sito protetto, che un giudice nazionale può, se il diritto interno lo consente, mantenere eccezionalmente gli effetti di simili misure, qualora tale mantenimento sia giustificato da considerazioni imperative connesse alla necessità di scongiurare una minaccia grave ed effettiva di interruzione dell'approvvigionamento di energia elettrica dello Stato membro interessato, cui non si potrebbe far fronte mediante altri mezzi e alternative, in particolare nell'ambito del mercato interno, potendo detto mantenimento però

coprire soltanto il lasso di tempo strettamente necessario per porre rimedio a tale illegittimità (v., in tal senso, sentenza del 29 luglio 2019, Inter-Environnement Wallonie e Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, punti 175, 176, 179 e 181).

100 Tuttavia, a differenza dell'omissione di un obbligo procedurale quale la valutazione preliminare dell'impatto di un progetto, che s'inserisce nell'ambito specifico della tutela dell'ambiente, una violazione dell'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, non può essere oggetto di regolarizzazione mediante una procedura analoga a quella menzionata al punto precedente (v., in tal senso, sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 121 e giurisprudenza ivi citata).

101 Infatti, il mantenimento degli effetti di una normativa nazionale come quella di cui ai procedimenti principali implicherebbe che detta normativa continui a imporre agli operatori di servizi di comunicazione elettronica obblighi che risultano contrari al diritto dell'Unione, e che comportano ingerenze gravi nei diritti fondamentali delle persone i cui dati sono stati conservati (v., per analogia, sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 122 e giurisprudenza ivi citata).

102 Pertanto, il giudice del rinvio non può limitare nel tempo gli effetti di una declaratoria di invalidità ad esso spettante, in forza del diritto nazionale, della legislazione nazionale di cui trattasi nei procedimenti principali (v., per analogia, sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 123 e giurisprudenza ivi citata).

103 Occorre inoltre precisare che nelle sentenze del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970), e del 6 ottobre 2020, La Quadrature du Net e a. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), non è stata operata una limitazione nel tempo degli effetti dell'interpretazione adottata sicché, conformemente alla giurisprudenza richiamata al punto 98 della presente sentenza, essa non può intervenire in una sentenza della Corte successiva a tali sentenze.

104 Infine, tenuto conto del fatto che il giudice del rinvio è investito di domande dirette a dichiarare irricevibili elementi di prova ottenuti a partire dai dati relativi al traffico, per il motivo che le disposizioni nazionali in questione sarebbero contrarie al diritto dell'Unione, sia per quanto riguarda la conservazione dei dati sia per quanto riguarda l'accesso ai medesimi, occorre determinare l'impatto della dichiarazione dell'eventuale incompatibilità dell'articolo L. 621-10 del CMF, nella versione applicabile ai fatti di cui ai procedimenti principali, con l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, sull'ammissibilità delle prove prodotte contro VD e SR nell'ambito dei procedimenti principali.

105 A tale riguardo, è sufficiente richiamare la giurisprudenza della Corte, in particolare i principi ricordati ai punti da 41 a 44 della sentenza del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche) (C-746/18, EU:C:2021:152), da cui discende che, conformemente al principio di autonomia procedurale degli Stati membri, tale ammissibilità rientra nell'ambito del diritto nazionale, fatto salvo il rispetto, in particolare, dei principi di equivalenza e di effettività.

106 Relativamente a quest'ultimo principio, occorre ricordare che esso impone al giudice penale nazionale di escludere informazioni ed elementi di prova, che siano stati ottenuti mediante una conservazione generalizzata e indiscriminata 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 di tale diritto, 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 a una materia estranea alla conoscenza dei giudici e idonei a influire in maniera preponderante sulla valutazione dei fatti [v., in tal senso, sentenza del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche), C-746/18, EU:C:2021:152, punto 44 e giurisprudenza ivi citata].

107 Tenuto conto delle considerazioni che precedono, occorre rispondere alle questioni pregiudiziali seconda e terza nelle presenti cause dichiarando che il diritto dell'Unione deve essere interpretato nel senso che esso osta a che un giudice nazionale limiti nel tempo gli effetti di una declaratoria di invalidità ad esso spettante, in forza del diritto nazionale, nei confronti delle disposizioni nazionali che, da un lato, impongono agli operatori di servizi di comunicazione elettronica una conservazione generalizzata e indiscriminata dei dati relativi al traffico e, dall'altro, consentono la comunicazione di simili dati all'autorità competente in materia finanziaria, senza previa autorizzazione di un organo giurisdizionale o di un'autorità amministrativa indipendente, a causa dell'incompatibilità di tali disposizioni con l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce della Carta. L'ammissibilità degli elementi di prova ottenuti in applicazione delle disposizioni legislative nazionali incompatibili con il diritto dell'Unione rientra, conformemente al principio di autonomia procedurale degli Stati membri, nell'ambito del diritto nazionale, fatto salvo il rispetto, in particolare, dei principi di equivalenza e di effettività.

## Sulle spese

108 Nei confronti delle parti nei procedimenti principali le presenti cause costituiscono 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 (Grande Sezione) dichiara:

**1) L'articolo 12, paragrafo 2, lettere a) e d), della direttiva 2003/6/CE del Parlamento europeo e del Consiglio, del 28 gennaio 2003, relativa all'abuso di informazioni privilegiate e alla manipolazione del mercato (abusi di mercato), e l'articolo 23, paragrafo 2, lettere g) e h), del regolamento (UE) n. 596/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, relativo agli abusi di mercato (regolamento sugli abusi di mercato) e che abroga la direttiva 2003/6 del Parlamento europeo e del Consiglio e le direttive 2003/124/CE, 2003/125/CE e 2004/72/CE della Commissione, in combinato disposto con l'articolo 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, e alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea,**

**devono essere interpretati nel senso che:**

**essi ostano a misure legislative che prevedono, a titolo preventivo, per finalità di contrasto dei reati di abuso di mercato, di cui fa parte l'abuso di informazioni privilegiate, una conservazione generalizzata e indiscriminata dei dati relativi al traffico per un anno a decorrere dal giorno della registrazione.**

2) **Il diritto dell'Unione deve essere interpretato nel senso che esso osta a che un giudice nazionale limiti nel tempo gli effetti di una declaratoria di invalidità ad esso spettante, in forza del diritto nazionale, nei confronti delle disposizioni nazionali che, da un lato, impongono agli operatori di servizi di comunicazione elettronica una conservazione generalizzata e indiscriminata dei dati relativi al traffico e, dall'altro, consentono la comunicazione di simili dati all'autorità competente in materia finanziaria, senza previa autorizzazione di un organo giurisdizionale o di un'autorità amministrativa indipendente, a causa dell'incompatibilità di tali disposizioni con l'articolo 15, paragrafo 1, della direttiva 2002/58, come modificata dalla direttiva 2009/136, letto alla luce della Carta dei diritti fondamentali dell'Unione europea. L'ammissibilità degli elementi di prova ottenuti in applicazione delle disposizioni legislative nazionali incompatibili con il diritto dell'Unione rientra, conformemente al principio di autonomia procedurale degli Stati membri, nell'ambito del diritto nazionale, fatto salvo il rispetto, in particolare, dei principi di equivalenza e di effettività.**

Firme