

CONCLUSIONI DELL'AVVOCATA GENERALE

LAILA MEDINA

presentate l'8 ottobre 2026

Causa C-222/25

X

contro

Rahapesu Andmehüroo,

parte interessata:

Andmekaitse Inspektsioon

[Domanda di pronuncia pregiudiziale proposta dalla Riigikohus (Corte suprema, Estonia)]

« Rinvio pregiudiziale – Protezione delle persone fisiche con riguardo al trattamento dei dati personali – Regolamento (UE) 2016/679 – Articolo 2, paragrafo 2, lettera d) – Direttiva (UE) 2016/680 – Articolo 1, paragrafo 1 – Ambito di applicazione – Nozione di “autorità competente” – Direttiva (UE) 2015/849 – Prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo – Unità di informazione finanziaria (FIU) – Trattamento di dati personali scambiati nel contesto di casi sospetti di riciclaggio – Diritto di accesso dell'interessato – Limitazioni previste da una misura legislativa – Accesso indiretto tramite un'autorità di controllo »

I. Introduzione

1. La criminalità, i proventi di reato e i flussi finanziari illeciti non conoscono frontiere. Negli ultimi decenni, l'Unione europea ha sviluppato una solida disciplina antiriciclaggio (in prosieguo: «AML») che mira anche a contrastare il finanziamento del terrorismo (in prosieguo: «CFT»). Tale disciplina è in costante evoluzione, in linea con gli sforzi intrapresi a livello internazionale in materia e, in particolare, con le raccomandazioni del Gruppo di azione finanziaria internazionale (GAFI) [\(2\)](#) e gli strumenti di altri organismi internazionali attivi nei settori AML/CFT [\(3\)](#). L'intelligence finanziaria e la condivisione di informazioni finanziarie costituiscono l'elemento cardine di tali sforzi. Le autorità nazionali competenti in materia di intelligence finanziaria, le Unità di informazione finanziaria [*Financial Intelligence Units*; in prosieguo: «FIU»), sono un elemento essenziale della disciplina internazionale e dell'Unione in materia di AML/CFT [\(4\)](#).

2. Nell'esercizio del loro compito principale di raccogliere, analizzare e comunicare informazioni di intelligence finanziaria, le FIU effettuano il trattamento di una grande quantità di dati personali. Nonostante i significativi poteri delle FIU e la quantità dei dati che trattano, il regime di protezione dei dati ad esse applicabile non è ancora del tutto chiaro. La presente causa offre alla Corte, per la prima volta, l'occasione di esaminare lo status giuridico delle FIU, il regime di protezione dei dati loro applicabile e le condizioni per la limitazione del diritto di accesso degli interessati ai dati personali di cui le FIU sono in possesso.

II. Fatti, procedimento nazionale e questioni pregiudiziali

3. X ha presentato due distinte richieste di informazioni, il 16 dicembre 2019 e il 27 dicembre 2019, al Rahapesu Andmehüüroo (Unità di informazione finanziaria, Estonia; in prosieguo: il «RAB»), al fine di accertare se fossero state trasmesse informazioni che lo riguardavano ad enti creditizi estoni o stranieri o ad autorità straniere e se questi ultimi avessero effettuato richieste in tal senso.

4. Il 20 dicembre 2019 e il 6 gennaio 2020 il RAB ha respinto queste due richieste, rispettivamente con la motivazione che, conformemente all'articolo 60, paragrafo 1, della Rahapesu ja terrorismi rahastamise tõkestamise seadus (legge sulla prevenzione del riciclaggio di denaro e del finanziamento del terrorismo), del 26 ottobre 2017 (RT I, 17.11.2017, 2; in prosieguo: la «RahaPTS») [\(5\)](#) e all'articolo 23, paragrafo 1, n. 1, dell'Avaliku teabe seadus (legge sull'informazione pubblica), del 15 novembre 2000 (RT I 2000, 92, 597; in prosieguo: la «AvTS») [\(6\)](#), esso non poteva divulgare i dati raccolti nell'esercizio delle proprie funzioni né informazioni circa l'esistenza o lo scambio di tali dati. In risposta alla successiva richiesta di X di precisare il motivo della limitazione dell'accesso, il RAB ha ribadito che, sulla base dell'articolo 60, paragrafo 1, della RahaPTS, esso non poteva confermare l'esistenza delle informazioni richieste né divulgarle.

5. Il Tallinna Halduskohus (Tribunale amministrativo di Tallinn, Estonia) e, in seguito, la Tallinna Ringkonnakohus (Corte d'appello di Tallinn, Estonia) hanno respinto il ricorso proposto da X avverso il rigetto delle sue richieste. Entrambe le sentenze sono state annullate dalla Riigikohus (Corte suprema, Estonia) che, con sentenza del 24 marzo 2022, ha ingiunto al RAB di adottare una nuova decisione sulle richieste di X.

6. In tale sentenza, la Riigikohus (Corte suprema) ha dichiarato che, ai sensi dell'articolo 41 della direttiva (UE) 2015/849 [\(7\)](#), e in assenza di un procedimento penale, il diritto di accesso di X ai dati che lo riguardano è disciplinato dal regolamento (UE) 2016/679 [\(8\)](#).

7. Essa ha altresì dichiarato che l'articolo 60, paragrafo 1, della RahaPTS non prevede, di per sé, una limitazione dei diritti dell'interessato, ma attribuisce al direttore del RAB il potere di limitare l'accesso a informazioni qualificandole come riservate ad uso interno. Orbene, nel caso di specie non era stata adottata una decisione di tal genere.

8. Nel frattempo, X ha presentato al RAB una terza richiesta di informazioni, al fine di accertare se quest'ultimo avesse avviato una pratica di verifica nei suoi confronti e se avesse sollecitato informazioni agli Stati Uniti d'America, richiesta anch'essa respinta dal RAB.

9. X ha quindi proposto un ricorso amministrativo dinanzi all'Andmekaitse Inspektsioon (Ispettorato per la protezione dei dati, Estonia; in prosieguo: l'«AKI»). L'AKI ha accolto il ricorso amministrativo e ha ingiunto al RAB di riesaminare la richiesta di informazioni. Il 17 febbraio 2022 il RAB ha nuovamente respinto la richiesta di informazioni, ragion per cui X ha presentato un nuovo ricorso amministrativo dinanzi all'AKI.
10. Con decisione del 18 aprile 2022, l'AKI ha emesso un provvedimento provvisorio con il quale ha ingiunto al RAB di fornire le informazioni richieste, dichiarando che i diritti dell'interessato non potevano essere limitati ai sensi dell'articolo 60, paragrafo 1, della RahaPTS.
11. Il 22 aprile 2022 il direttore del RAB ha adottato una decisione ai sensi dell'articolo 60, paragrafo 1, seconda frase, della RahaPTS, con cui ha limitato l'accesso di X, facendo presente di essere obbligato a mantenere riservate le informazioni contenute nella banca dati del RAB al fine di tutelare il sistema finanziario estone.
12. Il 13 maggio 2022, il direttore del RAB ha emanato un provvedimento che limitava l'accesso ai dati registrati nella banca dati del RAB con effetto retroattivo, dichiarando i dati di cui agli articoli da 8 a 17 del decreto del Ministro delle Finanze n. 56, del 16 dicembre 2020, relativo al Rahapesu Andmehüüri andmekogu põhimäärus (statuto della banca dati del RAB) [\(9\)](#) informazioni riservate ad uso interno della sola autorità (in prosieguo: il «provvedimento del direttore del RAB»).
13. Il 19 maggio 2022 il direttore del RAB ha adottato una decisione mediante la quale ha reiterato il rifiuto di dare seguito alla richiesta di informazioni di X, facendo riferimento all'articolo 23, paragrafo 1, n. 1, dell'AVTS e alle limitazioni all'accesso stabilite nella decisione del 22 aprile 2022 e nel provvedimento del direttore del RAB.
14. X ha impugnato le decisioni del 22 aprile 2022 e del 19 maggio 2022 nonché il provvedimento del direttore del RAB dinanzi al Tallinna Halduskohus (Tribunale amministrativo di Tallinn). Tale giudice ha accolto il ricorso con sentenza del 19 dicembre 2022. Esso ha ritenuto che l'articolo 60, paragrafo 1, della RahaPTS fosse incompatibile con l'articolo 23 del RGPD. A tal riguardo, esso ha sottolineato che l'articolo 60, paragrafo 1, della RahaPTS non precisa quali attività del RAB implicino il trattamento di dati personali, i motivi per i quali possono essere negate informazioni relative al trattamento di dati personali o la durata della limitazione. Esso ha quindi ingiunto al RAB di pronunciarsi nuovamente sulle richieste di informazioni di X.
15. Il RAB ha proposto ricorso dinanzi alla Tallinna Ringkonnakohus (Corte d'appello di Tallinn), che è stato respinto con sentenza del 10 aprile 2024. Tale giudice ha confermato la motivazione della sentenza impugnata, rilevando che l'articolo 60, paragrafo 1, della RahaPTS non è chiaro e preciso e che non consente alle persone interessate di conoscere la durata della limitazione. Esso ha inoltre ritenuto che le decisioni di cui trattasi e il provvedimento del direttore del RAB impugnato in questione stabiliscono una limitazione assoluta e illimitata del diritto di accesso, che non è proporzionata.

16. Il RAB ha proposto ricorso per cassazione avverso la sentenza della Tallinna Ringkonnakohus (Corte d'appello di Tallinn) dinanzi alla Riigikohus (Corte suprema), giudice del rinvio.

17. In primo luogo, il giudice del rinvio chiede alla Corte di chiarire quale regime di protezione dei dati si applichi ai dati trattati dal RAB, tenuto conto, da un lato, dell'articolo 41 della direttiva 2015/849, il quale stabilisce che il trattamento di dati effettuato ai sensi di tale direttiva è soggetto al RGPD, e, dall'altro, del considerando 40 della direttiva (UE) 2018/843 ([10](#)), ai sensi del quale la direttiva in parola si applica fatta salva la protezione dei dati personali trattati dalle autorità competenti a norma della direttiva (UE) 2016/680 ([11](#)).

18. Il giudice del rinvio precisa che il fatto che il RAB non sia un'autorità inquirente e non conduca procedimenti penali non dovrebbe necessariamente essere decisivo ai fini della delimitazione dell'ambito di applicazione del RGPD e della direttiva 2016/680, alla luce della sentenza della Corte nella causa La Quadrature du Net e a. (Dati personali e lotta contro la contraffazione) ([12](#)).

19. In secondo luogo, il giudice del rinvio chiede se, sulla base dell'articolo 23, paragrafo 2, lettera h), del RGPD o dell'articolo 15, paragrafo 3, della direttiva 2016/680, il RAB possa astenersi dall'indicare la base giuridica che giustifica un diniego di accesso. A tale riguardo, esso rileva l'assenza, nel RGPD, di un meccanismo per l'esercizio indiretto dei diritti dell'interessato tramite l'autorità di controllo competente, equivalente a quello previsto dall'articolo 17, paragrafo 1, della direttiva 2016/680.

20. In terzo luogo, il giudice del rinvio sottolinea che, sebbene una limitazione dei diritti dell'interessato mediante una misura legislativa sia ammessa indipendentemente dal fatto che nel caso specifico trovi applicazione il RGPD o la direttiva 2016/680, la misura legislativa in questione deve soddisfare i requisiti di chiarezza e precisione e la sua applicazione deve essere prevedibile.

21. Il giudice del rinvio rileva che l'articolo 60, paragrafo 1, della RahaPTS non indica espressamente i presupposti in presenza dei quali il direttore del RAB può adottare la decisione di limitare l'accesso alle informazioni, né l'ambito temporale o materiale di tale limitazione. La limitazione dei diritti dell'interessato potrebbe durare fino alla scadenza dei periodi di conservazione di cui all'articolo 26 dello statuto della banca dati del RAB (di regola, 15 anni). Decorso tale periodo, gli interessati perdono la possibilità di ottenere informazioni sui dati che li riguardano, perché tali dati sono cancellati.

22. Inoltre, la finalità della limitazione dell'accesso di cui all'articolo 60, paragrafo 1, seconda frase, della RahaPTS può essere determinata soltanto interpretando tale disposizione in combinato disposto con altre disposizioni della medesima legge e altri atti normativi in materia di prevenzione del riciclaggio e del finanziamento del terrorismo.

23. Infine, il giudice del rinvio chiede se l'articolo 23 del RGPD e l'articolo 15 della direttiva 2016/680 ostino a una normativa nazionale che limita totalmente l'esercizio del diritto di accesso ai dati personali sino alla loro distruzione.

24. In tali circostanze, la Riigikohus (Corte suprema) ha deciso di sospendere il procedimento e di sottoporre alla Corte di giustizia le seguenti questioni pregiudiziali:

«1) Se l'articolo 2, paragrafo 2, lettera d), del [RGPD] e l'articolo 2, paragrafo 1, in combinato disposto con il precedente articolo 1, della [direttiva 2016/680] debbano essere interpretati nel senso che l'eventuale trattamento di dati personali da parte di [una FIU] possa costituire un trattamento di dati personali da parte dell'autorità competente a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, compresa la salvaguardia e la prevenzione di minacce alla sicurezza pubblica, sebbene tale [FIU] non costituisca un'autorità inquirente ai sensi del codice di procedura penale.

2) Se l'articolo 23, paragrafo 2, lettera h), del RGPD e l'articolo 15, paragrafo 3, della direttiva 2016/680 debbano essere interpretati nel senso che ad un interessato, in un procedimento amministrativo o giudiziario, possa essere negata anche la comunicazione dell'atto giuridico in base al quale gli sia stato negato l'accesso a propri dati personali, al fine di evitare che il fatto del trattamento dei dati personali riguardanti la sua persona risulti confermato o smentito, qualora l'interessato medesimo non sia a conoscenza dell'esistenza o meno di tale trattamento, e se, in tal caso, possa essere parimenti omessa la comunicazione all'interessato della possibilità di invocare la misura di cui all'articolo 17, paragrafo 1, della direttiva 2016/680.

3) Se l'articolo 15 della direttiva 2016/680 o, rispettivamente, l'articolo 23 del RGPD debbano essere interpretati nel senso della loro compatibilità con una normativa nazionale che autorizzi il responsabile di [una FIU] a limitare i diritti dell'interessato e dalla quale emergano la *ratio*, le condizioni e l'ambito temporale e territoriale della restrizione dei diritti dell'interessato, in combinato disposto con altre normative, anche di grado subordinato.

4) Se l'articolo 15 della direttiva 2016/680 e l'articolo 23 del RGPD debbano essere interpretati nel senso della loro compatibilità con una normativa nazionale che restringa *in toto*, sino alla distruzione dei dati, l'esercizio del diritto previsto dall'articolo 14 della direttiva 2016/680 e dall'articolo 15 del RGPD, in modo che risulti impossibile per l'interessato ottenere l'accesso ai dati medesimi».

25. Hanno presentato osservazioni scritte il ricorrente nel procedimento principale, la Repubblica di Estonia, il Regno di Spagna, la Repubblica di Finlandia e la Commissione europea. La Repubblica di Estonia, il Regno di Spagna, la Repubblica francese, la Repubblica di Lettonia, il Granducato di Lussemburgo, il Regno dei Paesi Bassi, la Repubblica di Finlandia e la Commissione hanno partecipato all'udienza tenutasi il 3 giugno 2026 e hanno risposto oralmente ai quesiti formulati dalla Corte.

III. Valutazione

A. Prima questione (disciplina dell'Unione in materia di protezione dei dati applicabile alle FIU)

26. Con la sua prima questione, il giudice del rinvio chiede, in sostanza, se l'articolo 2, paragrafo 2, lettera d), del RGPD e l'articolo 2, paragrafo 1, della direttiva 2016/680, letti in

combinato disposto con l'articolo 1, paragrafo 1, di quest'ultima, debbano essere interpretati nel senso che il trattamento di dati personali da parte di una FIU, quale il RAB, possa essere considerato effettuato da un'autorità competente a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse, anche qualora la FIU in questione non sia un'autorità inquirente ai sensi del codice di procedura penale nazionale.

27. La questione mira a determinare quale disciplina dell'Unione in materia di dati sia applicabile a una FIU allorché svolge i compiti ad essa attribuiti nei settori AML/CFT. Tale accertamento riveste particolare importanza alla luce delle differenze tra il RGPD e la direttiva 2016/680. Ai fini della presente causa, è importante rilevare le differenze nella portata delle limitazioni dei diritti dell'interessato ([13](#)), il ruolo dell'autorità di controllo ai sensi dell'articolo 17 della direttiva 2016/680 relativamente all'esercizio indiretto dei diritti dell'interessato, nonché le differenze nel regime applicabile ai trasferimenti di dati verso paesi terzi o organizzazioni ([14](#)).

28. La questione centrale per determinare quale protezione dei dati sia applicabile è se il trattamento di dati da parte di una FIU, quale il RAB, debba essere considerato un trattamento effettuato da un'«autorità competente» ai sensi della direttiva 2016/680. In tale ipotesi, il trattamento di dati da parte del RAB rientrerebbe nell'ambito di applicazione *ratione materiae* della direttiva 2016/680, conformemente all'articolo 2, paragrafo 1, e all'articolo 1, paragrafo 1, di quest'ultima. Per analizzare tale questione, effettuerò anzitutto una breve panoramica dei criteri per la delimitazione dell'ambito di applicazione del RGPD e della direttiva 2016/680. Esaminerò quindi lo status, i compiti e le funzioni delle FIU, per poi giungere a una conclusione relativamente a quale regime di protezione dei dati sia applicabile alle FIU nell'esercizio dei loro compiti principali nel settore AML/CFT.

1. **Delimitazione dell'ambito di applicazione del RGPD e della direttiva 2016/680**

29. Il diritto fondamentale alla protezione dei dati personali è sancito all'articolo 8 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta») e dall'articolo 16, paragrafo 1, TFUE. La disciplina dell'Unione in materia di protezione dei dati si regge su tre pilastri: il RGPD, la direttiva 2016/680 e il regolamento (UE) 2018/1725 ([15](#)), che è applicabile alle istituzioni dell'Unione.

30. Come suggerito dalla sua denominazione, il RGPD istituisce un regime generale e orizzontale di protezione dei dati ([16](#)). L'articolo 2, paragrafo 2, del RGPD prevede quattro eccezioni all'ambito di applicazione di tale regolamento, quale definito al suo articolo 2, paragrafo 1, eccezioni che devono essere interpretate restrittivamente ([17](#)).

31. In particolare, l'articolo 2, paragrafo 2, lettera d), del RGPD esclude dal suo ambito di applicazione i trattamenti di dati personali effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

32. Come risulta dal considerando 19 del RGPD, tale eccezione è motivata dalla circostanza che i trattamenti di dati personali da parte delle autorità competenti per le succitate finalità sono disciplinati da un atto specifico dell'Unione, ossia la direttiva 2016/680, la quale è stata adottata il medesimo giorno del RGPD ([18](#)).

33. L'ambito di applicazione della direttiva 2016/680, previsto all'articolo 2, paragrafo 1, in combinato disposto con l'articolo 1, paragrafo 1, della stessa, è determinato sulla base della persona o del soggetto che effettua il trattamento e delle finalità del trattamento stesso ([19](#)). Il soggetto che effettua l'operazione deve essere un'«autorità competente» ai sensi dell'articolo 3, punto 7, della direttiva 2016/680. Nelle finalità del trattamento rientrano la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

34. Dal considerando 10 della direttiva 2016/680 risulta che la nozione di «autorità competente» deve essere intesa in relazione alla protezione dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia, tenuto conto degli adeguamenti che possono al riguardo risultare necessari in considerazione della specificità di tali settori. ([20](#)).

35. La definizione di «autorità competente» è contenuta nell'articolo 3, punto 7, della direttiva 2016/680.

36. L'articolo 3, punto 7, della direttiva 2016/680 prevede due categorie di autorità competenti. Al punto 7, lettera a), di tale disposizione, l'«autorità competente» è definita come «qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica». Tale definizione include le autorità pubbliche, quali le autorità giudiziarie, la polizia o altre autorità incaricate dell'applicazione della legge ([21](#)).

37. L'articolo 3, punto 7, lettera b), estende la definizione di autorità competente a «qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica».

38. La definizione di autorità competente deve essere applicata, per analogia, all'articolo 2, paragrafo 2, lettera d), del RGPD e all'eccezione in materia di attività di contrasto prevista da tale disposizione ([22](#)). Dalla formulazione della disposizione in parola risulta chiaramente che, ai fini dell'applicazione di tale eccezione, le due condizioni relative alle finalità del trattamento e al suo autore devono essere soddisfatte simultaneamente ([23](#)).

39. Pertanto, il fatto che il trattamento dei dati sia effettuato ai fini di attività di contrasto non è sufficiente, di per sé, ad escludere l'applicazione del RGPD ([24](#)). Di converso, il fatto che un'autorità competente effettui un trattamento di dati non è sufficiente a determinare l'applicazione della direttiva 2016/680 se detto trattamento non ha alcun rapporto con le finalità di contrasto ([25](#)).

40. La giurisprudenza della Corte fornisce esempi didascalici di delimitazione dell'ambito di applicazione dei due strumenti giuridici. La Corte ha dichiarato che, nell'esercizio di un'attività consistente nel comunicare al pubblico dati personali riguardanti i punti di penalità inflitti ai conducenti di veicoli per infrazioni stradali a fini di sicurezza stradale, l'entità lettone competente (26) non poteva essere considerata un'«autorità competente», ai sensi dell'articolo 3, punto 7, della direttiva 2016/680. Siffatta attività rientra, quindi, nell'ambito di applicazione materiale del RGPD (27). La Corte ha altresì statuito che, quando l'amministrazione tributaria raccoglie dati presso un operatore economico ai fini della riscossione delle imposte e della lotta all'evasione fiscale, essa non può essere considerata un'«autorità competente» ai sensi dell'articolo 3, punto 7, della direttiva 2016/680 (28).

41. Di converso, la Corte ha statuito che il trattamento dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi da parte di un'unità d'informazione sui passeggeri (UIP), un'autorità competente in materia di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, istituita dalla direttiva (UE) 2016/681 (29), rientra nell'ambito di applicazione della direttiva 2016/680 (30).

42. La Corte ha altresì statuito che la direttiva 2016/680 si applica ai trattamenti di dati effettuati dalla Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (autorità pubblica francese competente in materia di diffusione delle opere e la protezione dei diritti su Internet; Hadopi), quando tale autorità adotta misure nell'ambito del procedimento di «risposta graduata», poiché dette misure hanno carattere prepenale direttamente connesso al procedimento giudiziario (31).

43. Da tale giurisprudenza risulta che, per quanto riguarda la prevenzione dei reati, l'applicabilità della direttiva 2016/680 non dipende dalla questione se l'autorità pubblica interessata sia un'autorità inquirente ai sensi del diritto penale nazionale. Essa dipende dai compiti e dalle funzioni specifici dell'autorità pubblica di cui trattasi nell'ambito della catena di prevenzione dei reati, quali definiti dall'atto normativo che disciplina il trattamento dei dati da parte di detta autorità ai fini della prevenzione dei reati.

44. Alla luce delle considerazioni generali che precedono, esaminerò ora lo status, i compiti e le funzioni delle FIU nel contesto della disciplina AML/CFT, per poi valutare se esse soddisfino i criteri per l'applicazione della direttiva 2016/680.

2. *Status, compiti e funzioni delle FIU nel contesto della disciplina AML/CFT dell'Unione*

45. L'obbligo degli Stati membri di istituire le FIU è sancito all'articolo 32, paragrafo 1, della direttiva 2015/849 (nota anche come quarta direttiva antiriciclaggio).

46. Tuttavia, le FIU esistevano già molto tempo prima di essere formalmente riconosciute in tale direttiva (32). La decisione 2000/642/GAI del Consiglio (33), adottata nell'ambito dell'ex «terzo pilastro» relativo alla cooperazione di polizia e giudiziaria in materia penale (34), prevedeva, al suo articolo 1, paragrafo 1, l'obbligo, per gli Stati membri, di assicurarsi che «le [FIU] istituite o designate per ricevere informazioni finanziarie nel quadro della lotta al riciclaggio

dei proventi di attività illecite cooperino per raccogliere, analizzare e sottoporre a investigazione le informazioni nell'ambito delle [FIU] relative a ogni fatto che possa costituire indizio di riciclaggio, conformemente alle loro competenze nazionali». Ai sensi dell'articolo 3 di tale decisione, gli Stati membri erano tenuti ad assicurarsi che l'assolvimento delle funzioni delle FIU «non sia ostacolato dal loro statuto interno, che si tratti di autorità amministrative, di applicazione della legge o giudiziarie».

47. Lo status delle FIU varia da uno Stato membro all'altro (35). Il modello delle FIU non è stato oggetto di armonizzazione, poiché gli Stati membri restano «interamente responsabili per l'istituzione e la scelta della natura organizzativa delle FIU» (36).

48. La direttiva 2015/849, tuttavia, stabilisce un requisito essenziale che si applica indipendentemente dallo status della FIU scelto da ciascuno Stato membro. La FIU, ai sensi dell'articolo 32, paragrafo 3, della direttiva 2015/849, deve essere «autonoma e operativamente indipendente», nel senso che essa dovrebbe avere «l'autorità e la capacità di svolgere liberamente le sue funzioni, compresa la capacità di decidere autonomamente di analizzare, richiedere e disseminare informazioni specifiche».

49. Inoltre, la varietà degli status giuridici delle FIU non dovrebbe ostacolare la loro cooperazione (37) e l'efficacia dello scambio di informazioni tra le autorità di contrasto, le procure o le FIU (38).

50. Il compito principale di una FIU (39), enunciato all'articolo 32, paragrafo 1, della direttiva 2015/849, consiste nel «prevenire, individuare e combattere efficacemente il riciclaggio e il finanziamento del terrorismo». A tal fine, conformemente all'articolo 32, paragrafo 3, della direttiva 2015/849, la FIU è l'unità nazionale centrale incaricata di ricevere (40) e analizzare le segnalazioni di operazioni sospette ed altre informazioni che riguardano attività di riciclaggio, reati presupposto associati o attività di finanziamento del terrorismo. Essa ha inoltre la responsabilità di comunicare alle autorità competenti i risultati delle sue analisi e qualsiasi altra informazione pertinente qualora vi siano motivi di sospettare attività di riciclaggio, reati presupposto associati o attività di finanziamento del terrorismo.

51. Dall'articolo 32, paragrafo 4, della direttiva 2015/849 risulta che, nell'esercizio dei loro compiti e delle loro funzioni, le FIU dispongono di importanti poteri di accesso alle informazioni «investigative necessarie per assolvere i propri compiti in modo adeguato» (41).

52. Ai sensi dell'articolo 32, paragrafo 7, della direttiva 2015/849, alle FIU è altresì attribuito il potere, «in presenza del sospetto che un'operazione sia collegata ad attività di riciclaggio o di finanziamento del terrorismo, (...) di intraprendere (...) azioni urgenti per sospendere o rifiutare il consenso all'esecuzione dell'operazione allo scopo di analizzare l'operazione, confermare il sospetto e disseminare i risultati dell'analisi alle autorità competenti».

53. I compiti, le funzioni e i poteri delle FIU dimostrano la loro importanza nell'accertamento e nella prevenzione dei reati nei settori AML/CFT. Le FIU sono incaricate sia del compito di prevenire e contrastare il riciclaggio e il finanziamento del terrorismo, che rientra nelle attività di contrasto, sia di cooperare strettamente con le autorità di contrasto competenti (42).

54. Le FIU hanno uno status *sui generis*. Sebbene operino nel «più ampio settore delle attività di polizia» (43), non sono necessariamente integrate nelle strutture di polizia. Senza voler negare l'importanza delle FIU ai fini della garanzia del buon funzionamento del mercato finanziario dell'Unione (che giustifica il ricorso all'articolo 114 TFUE per l'adozione della direttiva 2015/849), occorre sottolineare che il loro ruolo nello scambio di informazioni finanziarie con le autorità di contrasto e con Europol è disciplinato in uno strumento di cooperazione di polizia fondato sull'articolo 87, paragrafo 2, TFUE, ossia la direttiva 2019/1153 (che ha sostituito la decisione 2000/642, uno strumento appartenente all'ex «terzo pilastro»).

55. I compiti, le funzioni e i poteri principali delle FIU indicano che il regime dell'Unione applicabile al trattamento di dati da parte di una FIU deve essere quello più adeguato alle finalità di contrasto. Lo illustrerò di seguito.

3. *Disciplina in materia di protezione dei dati applicabile alle FIU*

56. Tutti i governi che hanno preso posizione sulla questione del regime dell'Unione in materia di protezione dei dati applicabile alle FIU (44) hanno ritenuto, nelle loro osservazioni scritte o in udienza, che le FIU, nell'esercizio del loro compito principale, siano «autorità competenti» ai sensi della direttiva 2016/680. A tal riguardo, ai fini dell'interpretazione di tale direttiva, essi adottano, in sostanza, un approccio funzionale, incentrato sui compiti e sulle funzioni svolte dalle FIU.

57. Concordo sul fatto che il trattamento di dati personali da parte delle FIU, nell'esercizio dei loro compiti e delle loro funzioni principali, rientri nell'ambito di applicazione della direttiva 2016/680.

58. Come ho già precisato, il compito principale delle FIU concerne l'individuazione e la prevenzione dei reati nei settori AML/CFT. L'articolo 83, paragrafo 1, TFUE include il terrorismo e il riciclaggio di denaro tra le sfere di criminalità particolarmente grave che presentano una dimensione transnazionale, in relazione alle quali la normativa dell'Unione può stabilire norme minime relative alla definizione dei reati e delle sanzioni (45). Nello svolgimento di tale compito, le FIU partecipano alla prevenzione e all'individuazione dei reati di cui trattasi.

59. Come ho già osservato in precedenza, nell'ambito dei loro compiti le FIU intrattengono stretti rapporti con le autorità di contrasto e con Europol. Esse comunicano i risultati delle loro analisi alle autorità di contrasto, rispondono alle richieste di informazioni provenienti da tali autorità e hanno accesso esse stesse alle informazioni investigative di cui necessitano.

60. Le FIU occupano una posizione intermedia tra le entità del settore privato soggette agli obblighi di segnalazione antiriciclaggio, vale a dire, da un lato, i soggetti obbligati, e, dall'altro, le autorità di contrasto. Tuttavia, il loro ruolo non si limita alla semplice ricezione e trasmissione di informazioni. Il valore aggiunto delle FIU risiede nella loro analisi delle informazioni (46), che è fondamentale nella catena di prevenzione dei reati. Tenendo conto del loro ruolo in tale analisi e dei canali di scambio e comunicazione a loro disposizione, le FIU sono gli «hub dell'intelligence finanziaria» (47) dell'Unione europea, come efficacemente osservato dalla dottrina giuridica, e, in quanto tali, svolgono un ruolo fondamentale nell'assetto dell'AML/CFT.

61. Esse si collocano al crocevia (48) tra le attività di prevenzione, da un lato, e di indagine e perseguimento dei reati svolte dalle autorità di contrasto, dall'altro, nell'ambito del sistema nazionale di AML/CFT. Il compito principale di una FIU, come ha affermato il governo lettone in udienza, è nella fase iniziale del procedimento penale. Nello stesso ordine di idee, il governo lussemburghese ha correttamente rilevato che le FIU svolgono una funzione «prepenale», che si inserisce in un «*continuum* funzionale» che sfocia nell'applicazione della legge.

62. Tenuto conto del ruolo delle FIU nell'individuazione e nella prevenzione dei reati, taluni governi che hanno partecipato alla fase scritta del procedimento e all'udienza hanno tracciato un'analogia con le conclusioni della Corte nella sentenza *La Quadrature du Net e a. (Dati personali e lotta contro la contraffazione)* (49) in merito all'autorità francese Hadopi. In tale causa, come ho già rilevato in precedenza (50), la Corte ha dichiarato che l'Hadopi, un'autorità amministrativa che ha il potere di adottare misure di carattere «prepenale», deve essere qualificata come un'«autorità competente» ai sensi dell'articolo 3 della direttiva 2016/680, in quanto coinvolta in attività di prevenzione, indagine, accertamento e perseguimento di reati, vale a dire la contravvenzione per negligenza grave o il reato di contraffazione, e rientra quindi nell'ambito di applicazione di tale direttiva conformemente al suo articolo 1 (51). E ciò nonostante il fatto che la Corte abbia constatato che, in forza del diritto nazionale applicabile, la Hadopi «non dispone di poteri decisionali propri» (52).

63. Se il trattamento di dati da parte di un'autorità amministrativa come l'Hadopi rientra nell'ambito di applicazione della direttiva 2016/680, la stessa conclusione dovrebbe valere, *a fortiori*, per una FIU, un'autorità pubblica che, indipendentemente dal suo status ai sensi del diritto nazionale, è competente ad adottare decisioni autonome in materia di analisi, richiesta e comunicazione di informazioni di intelligence finanziaria e dispone di importanti poteri conferiti dal diritto dell'Unione necessari ai fini dell'individuazione e della prevenzione dei reati nei settori AML/CFT.

64. La maggior parte dei governi ha sottolineato, a mio avviso correttamente, il carattere analogo dei compiti delle FIU e dei compiti delle UIP (53), che la Corte, nella sentenza *Ligue des droits humains* (54), ha qualificato come «autorità competenti» rientranti nell'ambito di applicazione della direttiva 2016/680. Le UIP sono state qualificate come tali in ragione della loro competenza, derivante dagli articoli 4 e 7 della direttiva PNR, in materia di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi. Le UIP raccolgono dati PNR presso i vettori aerei, li trattano e trasferiscono tali dati o i risultati del loro trattamento alle autorità competenti. Inoltre, esse sono incaricate di scambiare sia i dati PNR che i risultati del trattamento di tali dati con le UIP degli altri Stati membri e con Europol. Le UIP rientrano chiaramente nell'ambito penale e si inseriscono nella catena di prevenzione e di accertamento dei reati.

65. La funzione delle FIU nella catena di prevenzione dei reati è simile a quella delle UIP, in quanto anch'esse ricevono informazioni, le analizzano e le comunicano alle autorità di contrasto.

66. La giurisprudenza della Corte, quindi, consente di concludere che il trattamento di dati da parte delle FIU ai fini della prevenzione dei reati nei settori AML/CFT rientra nell'ambito di applicazione della direttiva 2016/680.

67. Le FIU soddisfano anche il requisito relativo all'«autorità competente», di cui all'articolo 3, punto 7, lettera a), della direttiva 2016/680. Come rilevato in precedenza ([55](#)), tale definizione non include soltanto le autorità giudiziarie o di contrasto «tradizionali», ma si estende a «qualsiasi autorità pubblica» (il corsivo è mio) che dispone di competenze nel settore delle attività di contrasto.

68. La qualificazione di una FIU come «autorità competente» ai sensi dell'articolo 3, punto 7, della direttiva 2016/680 non dovrebbe dipendere dalla struttura organizzativa scelta (di contrasto, giudiziario, amministrativo o ibrido), bensì dai compiti e dalle funzioni che le sono conferiti e dai poteri che esercita. Non è decisivo nemmeno il fatto che una FIU, quale il RAB, non sia un'autorità inquirente ai sensi del codice di procedura penale nazionale ([56](#)).

69. Anche qualora si ritenga che una FIU non rientri nell'ambito dell'articolo 3, punto 7, lettera a), della direttiva 2016/680, come affermato dal governo lussemburghese, essa dovrebbe comunque essere considerata rientrante nell'ambito del punto 7, lettera b), di tale disposizione, che si applica a «qualsiasi altro organismo o entità» investiti di compiti in materia di attività di contrasto. Nella misura in cui, ai sensi dell'articolo 3, paragrafo 7, lettera b), di tale direttiva, un soggetto privato può essere qualificato come «autorità competente» quando è incaricato dal diritto di uno Stato membro di esercitare poteri di contrasto, ciò dovrebbe valere a maggior ragione per una FIU, che è un'autorità pubblica dotata di importanti poteri in materia di AML/CFT.

70. Ne consegue che una FIU deve essere qualificata come «autorità competente», ai sensi dell'articolo 3, punto 7, della direttiva 2016/680, allorché svolge i suoi compiti principali nei settori AML/CFT.

71. Ciò non pregiudica l'applicazione del RGPD quando le FIU trattano dati nell'esercizio di altri compiti loro affidati dal diritto nazionale, che non riguardano una delle attività previste dall'articolo 1, paragrafo 1, della direttiva 2016/680. Dall'articolo 9, paragrafo 2, di tale direttiva discende che il RGPD dovrebbe applicarsi al trattamento effettuato per tali altre finalità. Il governo estone ha sostenuto che il RAB dispone di una competenza di vigilanza nel settore non finanziario e che esso controlla altresì l'esecuzione di determinate sanzioni finanziarie. Pertanto, quando una FIU effettua il trattamento di dati per finalità non correlate al suo compito principale nei settori AML/CFT, tale trattamento rientra nell'ambito di applicazione del RGPD ([57](#)).

72. Ciononostante, la Commissione ritiene che le FIU non siano «autorità competenti» ai sensi della direttiva 2016/680, sicché il trattamento di dati da parte di tali autorità rientrerebbe nell'ambito di applicazione del RGPD.

73. A tal riguardo, essa ritiene che l'attività delle FIU si limiti al «pretrattamento amministrativo» di tutte le informazioni che ricevono. Soltanto le autorità competenti alle quali

esse comunicano informazioni possono trarre conclusioni circa la natura penale o meno delle attività di cui trattasi.

74. Tenuto conto dei compiti, delle funzioni e dei poteri delle FIU, che sono già stati ampiamente illustrati, tale approccio non si concilia, a mio avviso, con il ruolo centrale delle FIU nella catena di prevenzione dei reati. Le FIU, come indicato dalla loro denominazione, sono vere e proprie piattaforme di intelligence, dotate della capacità di adottare decisioni autonome nel contesto dell'analisi delle informazioni pertinenti. I poteri delle FIU di accedere alle informazioni investigative necessarie per assolvere i loro compiti in modo adeguato (ai sensi dell'articolo 32, paragrafo 4, della direttiva 2015/849), di scambiare informazioni con altre FIU, con le autorità di contrasto e con Europol, e il potere di sospendere o rifiutare il consenso all'esecuzione di un'operazione indicano chiaramente che il loro ruolo non è circoscritto a un mero pretrattamento amministrativo.

75. Il fatto che le FIU siano collocate in una posizione intermedia nella catena di accertamento e prevenzione dei reati e che comunichino informazioni alle autorità competenti non osta alla loro classificazione come «autorità competenti». Infatti, detta classificazione non dipende dall'esatta collocazione dell'autorità nell'ambito del sistema di contrasto alla criminalità, bensì dai suoi compiti e dalle sue funzioni (58).

76. L'argomento più forte avanzato dalla Commissione riguarda la formulazione dell'articolo 41, paragrafo 1, della direttiva 2015/849, il quale stabilisce che il trattamento dei dati personali ai sensi di tale direttiva è soggetto al RGPD. La Commissione osserva che tale disposizione è formulata in modo ampio, così da includere tutte le operazioni di trattamento ai sensi della direttiva 2015/849, comprese quelle effettuate dalle FIU.

77. Tuttavia, come sostenuto da quasi tutti i governi che hanno presentato osservazioni scritte e che hanno partecipato all'udienza (59), l'articolo 41, paragrafo 1, della direttiva 2015/849 dovrebbe essere interpretato facendo salva l'applicazione della direttiva 2016/680.

78. Il legislatore dell'Unione ha istituito un insieme completo di norme in materia di protezione dei dati che devono essere applicate in modo coerente in tutti i settori del diritto dell'Unione. Il RGPD e la direttiva 2016/680 sono applicabili ciascuno nel contesto del proprio ambito di applicazione. In altri termini, come dichiarato dal governo spagnolo in udienza, l'articolo 41, paragrafo 1, della direttiva 2015/849 non modifica le condizioni relative ai rispettivi ambiti di applicazione del RGPD e della direttiva 2016/680.

79. Ciò è confermato dal considerando 42 della direttiva 2015/849, ai sensi del quale quest'ultima lascia impregiudicata la protezione dei dati personali trattati nel quadro della cooperazione di polizia e giudiziaria in materia penale, comprese le disposizioni della decisione quadro 2008/977/GAI del Consiglio (60), strumento che ha preceduto la direttiva 2016/680. Occorre ricordare che tale decisione quadro, abrogata dalla direttiva 2016/680, aveva un ambito di applicazione limitato nel settore della giustizia e della cooperazione di polizia, dato che essa riguardava soltanto i trattamenti transfrontalieri.

80. Come ha sostenuto il governo francese in udienza, dal considerando 22 della direttiva 2016/680 risulta evidente, inoltre, che il legislatore dell'Unione non ha inteso modificare la regola di delimitazione tra il RGPD e la direttiva 2016/680 nei settori AML/CFT. Tale considerando riguarda una serie di autorità pubbliche alle quali sono comunicati dati personali conformemente a un obbligo legale derivante dalla loro missione istituzionale e precisa che il trattamento di dati personali da parte di tali autorità pubbliche dovrebbe essere conforme alle norme in materia di protezione dei dati applicabili secondo le finalità del trattamento.

81. La necessità di garantire la coerenza tra la direttiva 2015/849 e il vigente quadro normativo dell'Unione in materia di protezione dei dati è da ultimo confermata dalla direttiva 2024/1640 (sesta direttiva antiriciclaggio), che abroga la direttiva 2015/849. La direttiva 2024/1640 non contiene più una disposizione espressa in merito al regime di protezione dei dati applicabile. Sebbene il considerando 122 indichi che il RGPD si applica al trattamento dei dati personali ai fini di tale direttiva, il medesimo considerando fa anche riferimento all'applicazione della direttiva 2016/680.

82. La Commissione ha espresso preoccupazioni in ordine al fatto che se le FIU fossero considerate «autorità competenti», ciò potrebbe comprometterne l'indipendenza rispetto alle autorità competenti alle quali comunicano informazioni.

83. Mi è difficile condividere le preoccupazioni della Commissione. Le FIU devono essere considerate «autorità competenti» al fine di determinare il regime dell'Unione applicabile in materia di protezione dei dati. Tale determinazione non pregiudica la loro indipendenza e autonomia operative, che devono essere garantite indipendentemente dal loro status organizzativo, anche quando la FIU è inserita nella struttura di un'altra autorità [\(61\)](#).

84. Un ultimo argomento a favore dell'applicazione della direttiva 2016/680 alle FIU, nello svolgimento dei loro compiti e delle loro funzioni nei settori AML/CFT, consiste nella necessità di salvaguardare la possibilità di un esercizio indiretto del diritto di accesso degli interessati tramite l'autorità di controllo, ai sensi dell'articolo 17 di tale direttiva. Come spiegherò più dettagliatamente nell'ambito della mia analisi della quarta questione pregiudiziale, il controllo indiretto tramite l'autorità di controllo costituisce una garanzia importante per compensare la possibilità di una limitazione totale del diritto di accesso ai sensi dell'articolo 15, paragrafo 1, della direttiva 2016/680.

85. Alla luce di tutto ciò che precede, l'articolo 2, paragrafo 2, lettera d), del RGPD e l'articolo 2, paragrafo 1, della direttiva 2016/680, letti in combinato disposto con l'articolo 1, paragrafo 1, di tale direttiva, devono essere interpretati nel senso che il trattamento di dati personali da parte di una FIU, quale il RAB, nell'esercizio del suo compito di prevenire, individuare e combattere il riciclaggio e il finanziamento del terrorismo, nonché alla luce delle sue funzioni e dei suoi poteri in tale ambito, deve essere considerato effettuato da un'autorità competente, ai sensi dell'articolo 3, punto 7, della direttiva 2016/680, anche qualora la FIU interessata non sia un'autorità inquirente ai sensi del codice di procedura penale nazionale. Il trattamento di tali dati rientra pertanto nell'ambito di applicazione della direttiva 2016/680.

86. Alla luce della risposta che propongo alla Corte di dare alla prima questione pregiudiziale, analizzerò le restanti questioni relative alle limitazioni del diritto di accesso dell'interessato sulla base delle disposizioni pertinenti della direttiva 2016/680, senza tener conto del RGDP.

B. Quarta questione

87. Con la sua quarta questione, che è opportuno esaminare in seconda battuta, il giudice del rinvio chiede, in sostanza, se l'articolo 15 della direttiva 2016/680 debba essere interpretato nel senso che esso osta a una disposizione nazionale che restringa *in toto*, sino alla distruzione dei dati, l'esercizio del diritto dell'interessato di accedere ai dati personali che lo riguardano in possesso di una FIU, in modo che risulti impossibile per l'interessato ottenere informazioni su tali dati.

88. L'articolo 15, paragrafo 1, della direttiva 2016/680 autorizza il legislatore nazionale, tenuto conto della specificità delle finalità per le quali è effettuato il trattamento di dati rientranti nell'ambito di applicazione di tale direttiva (specificità sulla quale il considerando 10 della medesima, in particolare, richiama l'attenzione), ad adottare misure legislative che limitino il diritto di accesso dell'interessato, a determinate condizioni. Il diritto di accesso può essere limitato «in tutto o in parte» «nella misura e per il tempo in cui tale limitazione totale o parziale costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica» al fine di garantire una serie di obiettivi di interesse generale, elencati in modo esaustivo alle lettere da a) a e) di tale disposizione. Tali obiettivi comprendono la necessità di «non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari» e di «non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati (...)».

89. Ai sensi dell'articolo 15, paragrafo 2, della direttiva 2016/680, gli Stati membri sono legittimati ad adottare misure legislative al fine di determinare le categorie di trattamenti rientranti, in tutto o in parte, in detti obiettivi.

90. L'articolo 41, paragrafo 4, della direttiva 2015/849 prevede un obbligo specifico per gli Stati membri di limitare il diritto di accesso degli interessati «[n]ell'applicare il divieto di comunicazione di cui all'articolo 39, paragrafo 1». Ai sensi della disposizione in parola, nell'applicare tale divieto gli Stati membri adottano misure legislative volte a limitare «in tutto o in parte», il diritto di accesso dell'interessato ai dati, alle condizioni ivi previste. Tali condizioni sono, in sostanza, identiche a quelle previste all'articolo 15, paragrafo 1, della direttiva 2016/680. Esse riguardano la necessità e la proporzionalità della limitazione parziale o totale e la necessità di garantire gli obiettivi di cui all'articolo 41, paragrafo 4, della direttiva 2015/849 (62).

91. Il divieto di comunicazione cui fa riferimento la frase introduttiva dell'articolo 41, paragrafo 4, della direttiva 2015/849 riguarda i soggetti obbligati, ai quali è vietato divulgare («tipping-off», secondo la terminologia utilizzata nella raccomandazione n. 21 del GAFI) il fatto che informazioni relative a operazioni sospette siano in corso di comunicazione, saranno o siano state comunicate a una FIU conformemente all'articolo 33 di tale direttiva (63).

92. Il riferimento al divieto di comunicazione sembra indicare che l'articolo 41, paragrafo 4, della direttiva 2015/849 disciplini specificamente le limitazioni del diritto di accesso degli interessati in riferimento alle informazioni detenute dai soggetti obbligati e il fatto che tali informazioni siano in corso di comunicazione, saranno o siano state comunicate a una FIU (o a un organo di autoregolamentazione). Tuttavia, per quanto riguarda il diritto di accesso ai dati detenuti da una FIU, occorre ricordare che tali autorità non ricevono informazioni soltanto dai soggetti obbligati, ma anche da altre fonti (autorità competenti nazionali ed estere, FIU di altri Stati membri ed Europol), con le quali, inoltre, scambiano informazioni. Le FIU inoltre producono intelligence finanziaria (64). A seguito dell'adozione della direttiva 2016/680, e tenuto conto dell'ampia formulazione delle richieste di accesso dell'interessato nel procedimento principale, sembra più opportuno esaminare le limitazioni del diritto di accesso alla luce dell'articolo 15 di tale direttiva. Tale disposizione ha una portata ampia e può applicarsi a tutti i dati e le informazioni in possesso delle FIU (65).

93. Dall'articolo 15, paragrafo 1, della direttiva 2016/680 risulta che la limitazione del diritto di accesso che gli Stati membri hanno il diritto di prevedere può essere «totale». Tuttavia, tale limitazione totale (o parziale) deve rispettare il principio di proporzionalità. Ai sensi di detta disposizione, la misura legislativa volta a limitare, in tutto o in parte, il diritto di accesso dell'interessato può essere adottata «nella misura e per il tempo in cui tale limitazione totale o parziale costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata». Qualsiasi limitazione deve pertanto essere circoscritta, per quanto concerne la sua portata e la sua durata, a quanto necessario e proporzionato (66).

94. A tal riguardo, occorre ricordare che il diritto di accesso ai dati di carattere personale è sancito all'articolo 8, paragrafo 2, della Carta. Tale diritto non è assoluto, ma deve essere considerato alla luce della sua funzione sociale.

95. Infatti, come risulta dall'articolo 52, paragrafo 1, della Carta, quest'ultima ammette limitazioni all'esercizio di tali diritti, purché tali limitazioni siano previste dalla legge, rispettino il contenuto essenziale di detti diritti e, in ottemperanza al principio di proporzionalità, siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui (67).

96. Nel contesto della direttiva 2015/849, la completa riservatezza delle informazioni costituisce un presupposto indispensabile per l'efficacia del regime AML/CFT istituito da tale direttiva (68). Inoltre, dal considerando 46 di tale direttiva risulta che l'accesso della persona interessata ad eventuali informazioni relative alla segnalazione di un'operazione sospetta comprometterebbe gravemente l'efficacia della lotta al riciclaggio e al finanziamento del terrorismo. Le informazioni sono riservate e devono rimanere tali lungo l'intera catena in cui si avvicinano i principali attori di tale sistema: i soggetti obbligati, in capo ai quali incombe un divieto di comunicazione; le FIU, che raccolgono e analizzano informazioni riservate; e le autorità di contrasto.

97. Tutti i governi che hanno presentato osservazioni scritte hanno sostenuto, in udienza, che il requisito della riservatezza è una caratteristica intrinseca del sistema AML/CFT ed è un elemento essenziale nella cooperazione delle FIU. Tali governi hanno sottolineato la sensibilità delle informazioni detenute dalle FIU, in quanto la mera conoscenza del fatto che i dati siano oggetto di trattamento potrebbe compromettere le analisi e le indagini in corso e consentire alle persone sospettate di dissimulare l'origine dei fondi.

98. Una limitazione totale del diritto di accesso alle informazioni detenute dalle FIU nell'ambito del loro compito principale risulta, pertanto, necessaria e adeguata per raggiungere gli obiettivi dei regimi AML/CFT.

99. Ciò premesso, occorre ricordare che, secondo una giurisprudenza costante, la proporzionalità di misure dalle quali risulti un'ingerenza nei diritti garantiti dall'articolo 8 della Carta richiede il rispetto dei requisiti di idoneità e di necessità nonché del requisito relativo al carattere proporzionato di tali misure rispetto all'obiettivo perseguito (69). Più specificamente, le deroghe alla protezione dei dati personali e le limitazioni di quest'ultima operano entro i limiti dello stretto necessario (70).

100. In particolare, secondo la giurisprudenza della Corte, qualsiasi normativa che determini un'ingerenza nel diritto alla protezione dei dati personali deve stabilire, in conformità al principio di proporzionalità, regole chiare e precise che disciplinino la portata e l'applicazione della misura in questione e fissare requisiti minimi, di modo che le persone i cui dati personali siano stati trattati dispongano di garanzie sufficienti, che consentano di proteggere efficacemente tali dati contro i rischi di abuso, nonché contro qualsiasi accesso e utilizzo illecito (71). Tale normativa dev'essere giuridicamente vincolante nell'ambito dell'ordinamento nazionale e, in particolare, indicare in quali circostanze e a quali condizioni una misura che preveda il trattamento di tali dati possa essere adottata, garantendo così che l'ingerenza sia limitata allo stretto necessario, in modo da non compromettere il conseguimento di un obiettivo di interesse pubblico (72).

101. Da tale giurisprudenza risulta che una limitazione assoluta e incondizionata del diritto di accesso alle informazioni detenute dalla FIU, che non preveda alcuna circostanza, condizione o garanzia ai fini dell'applicazione di tale limitazione, costituisce un'ingerenza ingiustificata nel diritto alla protezione dei dati, incompatibile con l'articolo 15, paragrafo 1, della direttiva 2016/680. In assenza di condizioni o criteri stabiliti per legge, né l'autorità di controllo né il giudice competente che esercita il controllo giurisdizionale sulla decisione del titolare del trattamento possono esaminare la legittimità della limitazione imposta.

102. Occorre altresì osservare che, ai sensi dell'articolo 15, paragrafo 4, della direttiva 2016/680, il titolare del trattamento è tenuto a documentare i motivi di fatto o di diritto su cui si basa la decisione di negare l'accesso, nonché a rendere disponibili tali informazioni alle autorità di controllo. L'obbligo del titolare del trattamento di documentare il diniego garantisce la responsabilità dello stesso dinanzi all'autorità di controllo e permette un controllo giurisdizionale effettivo (73). In altri termini, la possibilità, per il titolare del trattamento, di

rifiutare l'accesso dell'interessato non dà carta bianca al titolare del trattamento (nella fattispecie, alla FIU).

103. I requisiti di necessità e di proporzionalità, derivanti dall'articolo 52, paragrafo 1, della Carta, devono essere rispettati anche quando gli Stati membri determinano, conformemente all'articolo 15, paragrafo 2, della direttiva 2016/680, le categorie di trattamenti alle quali si applicano limitazioni ai sensi dell'articolo 15, paragrafo 1, di tale direttiva.

104. Per quanto riguarda la normativa nazionale di cui al procedimento principale, il giudice del rinvio ha dichiarato che essa prevede una limitazione assoluta del diritto di accesso di chiunque, in qualsiasi circostanza e sino alla distruzione dei dati. Il provvedimento del direttore del RAB, che limita l'accesso a tutti i dati contenuti nella banca dati del RAB, non sembra stabilire alcuna regola precisa che disciplini la portata e l'applicazione della limitazione dell'accesso, né imporre requisiti minimi per prevenire il rischio di abuso e garantire che la FIU applichi le limitazioni in questione nella misura strettamente necessaria. Come rilevato dalla Commissione nelle sue osservazioni scritte, in sostanza, la necessità e la proporzionalità della limitazione di tale diritto devono essere garantite sulla base di criteri generali che consentano di valutare ogni singola richiesta di accesso.

105. Il governo estone ha dichiarato, in udienza, che il contesto normativo nazionale non stabilisce una limitazione assoluta o categorica. Esso ha sostenuto che il direttore del RAB dispone di un potere discrezionale al fine di valutare e decidere su ciascuna richiesta di accesso. Esso ha confermato che tale potere è esercitato, ad esempio, quando una persona è già a conoscenza del fatto che è in corso un'indagine, oppure quando il RAB decide di congelare i fondi di tale persona.

106. Spetta al giudice del rinvio, che è competente a interpretare il proprio diritto nazionale, verificare se esistano, nel contesto giuridico nazionale, elementi atti a garantire che la limitazione del diritto di accesso si applichi soltanto nella misura strettamente necessaria per non compromettere la finalità di interesse pubblico per la quale è prevista la limitazione dell'accesso e che tale limitazione non sia arbitraria.

107. Ciò premesso, come correttamente rilevato dalla Commissione in udienza, anche qualora si ritenga che il direttore del RAB disponga di un margine di discrezionalità, gli elementi o i criteri che definiscono l'ambito di siffatta discrezionalità devono essere stabiliti nella rispettiva misura nazionale. Orbene, tali elementi non risultano dall'illustrazione della normativa nazionale pertinente.

108. Pertanto, sebbene il diritto nazionale possa prevedere una limitazione totale dell'accesso ai dati detenuti dalla FIU, esso deve stabilire regole chiare e precise che disciplinino la portata e le condizioni di applicazione della misura legislativa in questione e fissino requisiti minimi, di modo che le persone i cui dati personali sono trattati dispongano di garanzie sufficienti, che consentano di proteggere efficacemente tali dati contro i rischi di abuso, nonché contro qualsiasi accesso e utilizzo illecito da parte della FIU o di qualsiasi altra autorità competente nell'ambito dei sistemi AML/CFT ([74](#)).

109. Inoltre, qualsiasi limitazione totale dell'accesso imposta all'interessato deve essere controbilanciata dal meccanismo previsto all'articolo 17 della direttiva 2016/680. Tale disposizione prevede l'esercizio indiretto dei diritti dell'interessato da parte dell'autorità di controllo. Tale esercizio indiretto si applica, *inter alia*, nella situazione di cui all'articolo 15, paragrafo 3, della direttiva in parola, che riconosce al titolare del trattamento la facoltà di non informare l'interessato circa il rifiuto o la limitazione dell'accesso e i relativi motivi, qualora una simile informazione rischi di compromettere una delle finalità di interesse pubblico di cui all'articolo 15, paragrafo 1, di tale direttiva. Ai sensi dell'articolo 17, paragrafo 3, quando l'autorità di controllo esercita il diritto di accesso per conto dell'interessato, essa è tenuta ad informarlo, perlomeno, di aver effettuato tutte le verifiche necessarie o un riesame.

110. La giurisprudenza della Corte sottolinea l'importanza dell'esercizio indiretto dei diritti dell'interessato al fine di garantire che vi sia un adeguato equilibrio tra l'interesse pubblico che giustifica la limitazione del diritto di accesso e i diritti fondamentali dell'interessato alla protezione dei dati e a un controllo giurisdizionale effettivo ai sensi dell'articolo 47 della Carta. Nella sentenza *Ligue des droits humains* (Verifica del trattamento dei dati da parte dell'autorità di controllo), la Corte ha dichiarato che, come si evince dal considerando 48 della direttiva 2016/680, l'esercizio indiretto dei diritti dell'interessato tramite l'autorità di controllo competente deve essere considerato necessario per la tutela di tali diritti, in quanto il loro esercizio diretto presso il titolare del trattamento risulta difficile o addirittura impossibile (75).

111. Per quanto riguarda il ruolo preciso dell'autorità di controllo nell'esercizio indiretto di tali diritti, la Corte ha dichiarato che una simile autorità è tenuta a instaurare con il titolare del trattamento un dialogo riservato e, a seguito di tale dialogo, decidere quali siano le informazioni necessarie all'esercizio, da parte dell'interessato, del suo diritto a un ricorso giurisdizionale effettivo (76).

112. Inoltre, dalla giurisprudenza della Corte risulta che, nell'ambito del controllo giurisdizionale della corretta applicazione dell'articolo 17 della direttiva 2016/680, spetta agli Stati membri istituire norme che consentano al giudice competente di prendere conoscenza sia dell'insieme dei motivi sia degli elementi di prova pertinenti su cui l'autorità di controllo ha basato, in tale ambito, la verifica della liceità del trattamento dei dati di cui trattasi nonché le conclusioni che ne ha tratto (77). Le informazioni trasmesse dal titolare del trattamento all'autorità di controllo quanto ai motivi sui quali ha fondato la propria decisione devono essere rese disponibili anche all'organo giurisdizionale investito di un ricorso contro l'autorità di controllo (78).

113. In udienza, il governo estone ha sostenuto che l'autorità nazionale di controllo è competente a verificare la liceità del trattamento dei dati da parte del RAB. Spetta al giudice del rinvio verificare che il diritto nazionale garantisca la corretta applicazione dell'articolo 17 della direttiva 2016/680.

114. Alla luce di tutte le considerazioni che precedono, l'articolo 15 della direttiva 2016/680 deve essere interpretato nel senso che esso osta a una disposizione nazionale che restringe *in toto*, sino alla distruzione dei dati, l'esercizio del diritto dell'interessato di accedere ai dati personali che lo riguardano in possesso di una FIU, in modo che risulti impossibile per

l'interessato ottenere informazioni su tali dati, qualora la misura nazionale pertinente non stabilisca regole chiare e precise che disciplinino la portata e l'applicazione della misura in questione e non fissi requisiti minimi, di modo che le persone i cui dati personali sono trattati dispongano di garanzie sufficienti, che consentano di proteggere efficacemente tali dati contro i rischi di abuso, nonché contro qualsiasi accesso e utilizzo illecito da parte della FIU interessata.

C. Seconda questione

115. Secondo una giurisprudenza costante, nell'ambito della procedura di cooperazione tra le giurisdizioni nazionali e la Corte, istituita all'articolo 267 TFUE, spetta a quest'ultima fornire al giudice nazionale una risposta utile che gli consenta di dirimere la controversia di cui è investito. In tale prospettiva, la Corte deve, all'occorrenza, riformulare le questioni che le sono sottoposte [\(79\)](#).

116. Nel caso di specie, nella prima parte della sua seconda questione, il giudice del rinvio chiede se l'articolo 15, paragrafo 3, della direttiva 2016/680 consenta a una FIU di rifiutare la comunicazione all'interessato dell'atto giuridico in base al quale gli sia stato negato l'accesso a dati personali che lo riguardano, al fine di evitare che il trattamento dei dati riguardanti la sua persona risulti confermato o smentito.

117. Nelle sue osservazioni scritte, la Commissione ha sostenuto che la seconda questione è irricevibile. Essa ha affermato che la decisione del RAB di diniego di accesso nel procedimento principale faceva esplicito riferimento al fondamento normativo del diniego, vale a dire l'articolo 60, paragrafo 1, della RahaPTS e l'articolo 23, paragrafo 1, n. 1, dell'AVTS.

118. In udienza, il governo estone ha fatto valere che la questione è ricevibile, mentre il governo dei Paesi Bassi ha sostenuto che è inesatto suggerire che la comunicazione di un motivo di limitazione dell'accesso possa rivelare l'avvenuto trattamento di dati personali. In ogni caso, la limitazione del diritto di accesso permette di limitare le informazioni relative all'effettuazione o alla non effettuazione del trattamento.

119. Alla luce delle spiegazioni contenute nella decisione di rinvio, che fa riferimento, in termini generali, al «fondamento normativo» della limitazione ma anche ai «motivi di fatto o di diritto» delle decisioni riguardanti gli interessati, la prima parte della seconda questione può essere intesa nel senso che essa riguarda la circostanza se una FIU possa rifiutarsi di comunicare i motivi del diniego.

120. Pertanto, in applicazione della giurisprudenza citata al paragrafo 115 delle presenti conclusioni, si deve ritenere che, con la sua seconda questione, il giudice del rinvio chieda, in sostanza, se l'articolo 15, paragrafo 3, della direttiva 2016/680 debba essere interpretato nel senso che esso consente a una FIU di rifiutarsi di indicare i motivi del diniego o della limitazione al fine di evitare che il trattamento dei dati personali dell'interessato risulti confermato o smentito e se, in tal caso, possa essere parimenti omessa la comunicazione all'interessato della possibilità di esercitare il suo diritto di accesso tramite l'autorità di controllo, ai sensi dell'articolo 17, paragrafo 1, della direttiva 2016/680.

121. Ai sensi dell'articolo 15, paragrafo 3, della direttiva 2016/680, qualora si applichi una limitazione del diritto di accesso dell'interessato (80), il titolare del trattamento è tenuto a informare l'interessato, senza ingiustificato ritardo e per iscritto, di ogni rifiuto o limitazione dell'accesso e dei motivi del rifiuto o della limitazione. Detta comunicazione può essere omessa qualora il suo rilascio rischi di compromettere una delle finalità di interesse pubblico di cui all'articolo 15, paragrafo 1, di tale direttiva (81).

122. Da tale disposizione discende che, fatte salve le condizioni ivi stabilite, una FIU è autorizzata a fornire una risposta del tipo «non si conferma e non si smentisce» e di omettere di indicare se sia stato effettuato o meno un trattamento.

123. Tuttavia, dall'articolo 15, paragrafo 3, della direttiva 2016/680 risulta che il titolare del trattamento è tenuto, in tal caso, a informare l'interessato della possibilità di proporre reclamo dinanzi a un'autorità di controllo o di proporre ricorso giurisdizionale. Il titolare del trattamento è altresì tenuto, conformemente all'articolo 17, paragrafo 2, della direttiva 2016/680, a informare l'interessato della possibilità di esercitare i suoi diritti tramite l'autorità di controllo ai sensi del paragrafo 1 di tale articolo. Non è prevista alcuna deroga all'obbligo di fornire tale informazione.

124. Ciò in ragione dell'importanza fondamentale del diritto di accesso indiretto tramite l'autorità di controllo. Come già rilevato in precedenza nell'ambito dell'analisi della quarta questione (82), l'esistenza di tale diritto compensa il rifiuto del titolare del trattamento di fornire informazioni sul trattamento dei dati. Quando l'esercizio diretto del diritto di accesso è difficile o impossibile, l'interessato deve sempre essere informato della possibilità di esercitare i propri diritti indirettamente. Inoltre, una FIU non è esonerata dall'obbligo di documentare i motivi su cui si basa la decisione di diniego dell'accesso e di rendere disponibile tale informazione alle autorità di controllo, conformemente all'articolo 15, paragrafo 4, di tale direttiva (83).

125. Alla luce di quanto precede, l'articolo 15, paragrafo 3, della direttiva 2016/680 deve essere interpretato nel senso che esso consente a una FIU di rifiutare la comunicazione dei motivi del diniego o della limitazione al fine di evitare che il trattamento dei dati personali riguardanti l'interessato risulti confermato o smentito. Tuttavia, in una situazione del genere, gli interessati devono sempre essere informati della possibilità di esercitare il loro diritto di accesso tramite l'autorità di controllo ai sensi dell'articolo 17, paragrafo 1, della direttiva 2016/680.

D. Terza questione

126. Con la sua terza questione, il giudice del rinvio chiede, in sostanza, se l'articolo 15, paragrafo 1, della direttiva 2016/680 debba essere interpretato nel senso che esso osta a una normativa nazionale che attribuisca al responsabile di una FIU, mediante una disposizione generale, il potere di limitare i diritti degli interessati, qualora l'interpretazione della *ratio*, delle condizioni e della portata della limitazione debba essere effettuata in combinato disposto con altre disposizioni giuridiche, anche di grado subordinato.

127. Dall'articolo 15, paragrafo 1, della direttiva 2016/680 risulta che qualsiasi limitazione del diritto di accesso degli interessati esige l'adozione di una misura legislativa da parte degli Stati membri.

128. Dal considerando 33 di tale direttiva risulta che il riferimento a una misura legislativa non richiede necessariamente l'adozione di un atto legislativo da parte di un parlamento. Tuttavia, una simile misura legislativa deve essere chiara e precisa, e la sua applicazione prevedibile, per coloro che vi sono sottoposti, come richiesto dalla giurisprudenza della Corte di giustizia e della Corte europea dei diritti dell'uomo. Tale considerando precisa altresì che il diritto dello Stato membro che disciplina il trattamento dei dati personali dovrebbe specificare quanto meno gli obiettivi, i dati personali da trattare, le finalità del trattamento e le procedure per preservare l'integrità e la riservatezza dei dati personali come pure le procedure per la loro distruzione, fornendo in tal modo sufficienti garanzie contro il rischio di abuso e arbitrarietà.

129. Nella sua giurisprudenza, la Corte ha desunto dall'articolo 8, paragrafo 2, della Carta, che a sua volta si limita a riflettere, concretizzandolo, il requisito posto dall'articolo 52 della Carta secondo cui eventuali limitazioni all'esercizio dei diritti fondamentali riconosciuti da quest'ultima devono in particolare essere previste dalla legge, che qualsiasi base giuridica che consenta l'ingerenza nel diritto alla protezione dei dati personali deve definire essa stessa la portata della limitazione dell'esercizio di tale diritto che essa può comportare [\(84\)](#).

130. Inoltre, la Corte ha dichiarato, per quanto riguarda il requisito posto dall'articolo 52 della Carta, che qualsiasi ingerenza nel diritto alla protezione dei dati personali deve essere operata nel rispetto del principio di proporzionalità, il che richiede che qualsiasi normativa che determini una siffatta ingerenza stabilisca regole chiare e precise che disciplinino la portata e l'applicazione della misura in questione e fissino requisiti minimi, di modo che le persone i cui dati personali siano stati trattati dispongano di garanzie sufficienti, che consentano di proteggere efficacemente tali dati contro i rischi di abuso, nonché contro qualsiasi accesso e utilizzo illecito [\(85\)](#).

131. Dalla giurisprudenza della Corte, che rinvia alla giurisprudenza consolidata della Corte europea dei diritti dell'uomo, discende che l'espressione «previsto dalla legge» utilizzata all'articolo 8, paragrafo 2, della Carta deve essere intesa nella sua accezione sostanziale e non formale [\(86\)](#). Inoltre, dalla giurisprudenza della Corte europea dei diritti dell'uomo risulta che il termine «legge», nell'espressione «prevista dalla legge», di cui all'articolo 8, paragrafo 2, della CEDU, si riferisce non soltanto agli atti legislativi, ma anche alle disposizioni giuridiche di grado subordinato [\(87\)](#). Si riferisce al testo in vigore, come interpretato dagli organi giurisdizionali competenti [\(88\)](#).

132. Pertanto, il requisito enunciato all'articolo 15, paragrafo 1, della direttiva 2016/680, ai sensi del quale qualsiasi limitazione deve essere basata su misure legislative, dovrebbe essere inteso ampiamente, nel senso che esso non è soddisfatto soltanto in presenza di un unico atto legislativo che disciplini tutti gli aspetti della limitazione dell'accesso a una determinata categoria di dati, come i dati detenuti dal RAB. I termini «misure legislative» possono includere

un insieme di disposizioni legislative, comprese disposizioni di grado subordinato, come interpretate dagli organi giurisdizionali competenti.

133. Ciò a patto che, tuttavia, le misure legislative pertinenti permettano una comprensione chiara e precisa della portata della limitazione che impongono e che l'applicazione di tali misure sia prevedibile per coloro i quali vi sono sottoposti. L'applicazione di una misura adottata ai sensi della direttiva 2016/680 è prevedibile per le persone che vi sono sottoposte quando queste ultime sono in grado di individuare le circostanze e le condizioni in cui può essere limitata la portata dei diritti conferiti loro da tale direttiva [\(89\)](#).

134. Nel caso del procedimento principale, diverse misure legislative prevedono disposizioni rilevanti ai fini dell'esercizio del diritto di accesso. L'articolo 60, paragrafo 1, della RahaPTS consente al direttore del RAB di limitare l'accesso ai dati contenuti nella banca dati del RAB e di qualificarli come informazioni per uso interno. Il provvedimento del RAB del 13 maggio 2022 prevede una limitazione dell'accesso ai dati contenuti nella banca dati del RAB, qualificandoli come dati riservati ad uso interno. L'articolo 23, paragrafo 1, n. 1, dell'AVTS consente la limitazione dell'accesso ai dati qualora il richiedente non abbia il diritto di accedere a tali dati.

135. Tali disposizioni sembrano essere formulate in termini assai generici e non sembrano tali da permettere agli interessati di individuare le condizioni e le circostanze in cui è permessa una limitazione, né le garanzie che consentano di proteggere efficacemente tali dati contro i rischi di abuso, nonché contro qualsiasi accesso e utilizzo illecito [\(90\)](#).

136. È vero che la normativa che disciplina il RAB contiene talune informazioni rilevanti per il trattamento dei dati, segnatamente designando il titolare del trattamento (il RAB), il tipo di dati inseriti nella banca dati [\(91\)](#), la classificazione della sicurezza dei dati [\(92\)](#) e il periodo di tempo in cui i dati riguardanti una persona sono conservati nella banca dati [\(93\)](#).

137. Tuttavia, tali elementi riguardano, più in generale, il trattamento dei dati da parte del RAB, senza alcun riferimento specifico alle condizioni e alle circostanze della limitazione del diritto di accesso e alle garanzie contro il rischio di abusi.

138. In udienza, il governo estone ha dichiarato che il direttore del RAB dispone di un potere discrezionale al fine di decidere se concedere o meno l'accesso ai dati contenuti nella banca dati del RAB e che esistono circostanze in cui l'accesso può essere concesso. Tuttavia, come già rilevato in precedenza [\(94\)](#), il contesto normativo pertinente non sembra circoscrivere tale discrezionalità, né prevedere condizioni chiare e precise per la limitazione del diritto di accesso. Ciò corrobora la conclusione secondo cui le misure legislative nazionali pertinenti non sembrano soddisfare il requisito ai sensi del quale si deve trattare di regole chiare e precise la cui applicazione sia prevedibile per l'interessato che intenda esercitare il suo diritto di accesso, circostanza che spetta tuttavia al giudice nazionale valutare.

139. Alla luce di quanto precede, l'articolo 15, paragrafo 1, della direttiva 2016/680 deve essere interpretato nel senso che esso non osta a una normativa nazionale che attribuisca al responsabile di una FIU, mediante una disposizione generale, il potere di limitare i diritti degli interessati, per il solo motivo che la *ratio*, le condizioni e la portata della limitazione devono

essere interpretati in combinato disposto con altre disposizioni giuridiche, anche di grado subordinato. Tuttavia, la stessa disposizione osta a detta normativa nazionale qualora le disposizioni nazionali pertinenti non stabiliscano regole chiare e precise che disciplinino la portata e le condizioni di applicazione della limitazione del diritto di accesso, di modo che le persone i cui dati personali sono oggetto di trattamento dispongano di garanzie sufficienti, che consentano di proteggere efficacemente tali dati contro i rischi di abuso, nonché contro qualsiasi accesso e utilizzo illecito.

IV. Conclusione

140. Alla luce delle considerazioni che precedono, suggerisco alla Corte di rispondere nei seguenti termini alle questioni pregiudiziali proposte dalla Riigikohus (Corte suprema, Estonia):

1) L'articolo 2, paragrafo 2, lettera d), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) e l'articolo 2, paragrafo 1, della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, letti in combinato disposto con l'articolo 1, paragrafo 1, di tale direttiva,

devono essere interpretati nel senso che il trattamento di dati personali da parte di un'Unità di informazione finanziaria (FIU), quale il RAB, nell'esercizio del suo compito di prevenire, individuare e combattere il riciclaggio e il finanziamento del terrorismo, nonché alla luce delle sue funzioni e dei suoi poteri in tale ambito, deve essere considerato effettuato da un'autorità competente, ai sensi dell'articolo 3, punto 7, della direttiva 2016/680, anche qualora la FIU interessata non sia un'autorità inquirente ai sensi del codice di procedura penale nazionale. Il trattamento di tali dati rientra pertanto nell'ambito di applicazione della direttiva 2016/680.

2) L'articolo 15 della direttiva 2016/680

deve essere interpretato nel senso che esso osta a una disposizione nazionale che restringe *in toto*, sino alla distruzione dei dati, l'esercizio del diritto dell'interessato di accedere ai dati personali che lo riguardano in possesso di una FIU, in modo che risulti impossibile per l'interessato ottenere informazioni su tali dati, qualora la misura nazionale pertinente non stabilisca regole chiare e precise che disciplinino la portata e l'applicazione della misura in questione e non fissi requisiti minimi, di modo che le persone i cui dati personali sono trattati dispongano di garanzie sufficienti, che consentano di proteggere efficacemente tali dati contro i rischi di abuso, nonché contro qualsiasi accesso e utilizzo illecito da parte della FIU interessata.

3) L'articolo 15, paragrafo 3, della direttiva 2016/680

deve essere interpretato nel senso che esso consente a una FIU di rifiutare la comunicazione dei motivi del diniego o della limitazione al fine di evitare che il trattamento dei dati personali riguardanti l'interessato risulti confermato o smentito. Tuttavia, in una situazione del genere, gli interessati devono sempre essere informati della possibilità di esercitare il loro diritto di accesso tramite l'autorità di controllo ai sensi dell'articolo 17, paragrafo 1, della direttiva 2016/680.

4) L'articolo 15, paragrafo 1, della direttiva 2016/680

deve essere interpretato nel senso che esso non osta a una normativa nazionale che attribuisca al responsabile di una FIU, mediante una disposizione generale, il potere di limitare i diritti degli interessati, per il solo motivo che la *ratio*, le condizioni e la portata della limitazione devono essere interpretati in combinato disposto con altre disposizioni giuridiche, anche di grado subordinato. Tuttavia, la stessa disposizione osta a detta normativa nazionale qualora le disposizioni nazionali pertinenti non stabiliscano regole chiare e precise che disciplinino la portata e le condizioni di applicazione della limitazione del diritto di accesso, di modo che le persone i cui dati personali sono oggetto di trattamento dispongano di garanzie sufficienti, che consentano di proteggere efficacemente tali dati contro i rischi di abuso, nonché contro qualsiasi accesso e utilizzo illecito.

[1](#) Lingua originale: l'inglese.

[2](#) Il GAFI è un organismo intergovernativo che definisce norme ed elabora e promuove politiche volte a combattere il riciclaggio e il finanziamento del terrorismo.

[3](#) V. considerando 4 del regolamento (UE) 2024/1624 del Parlamento europeo e del Consiglio, del 31 maggio 2024, relativo alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo (GU L, 2024/1624); Mitsilegas, V. e Vavoula, N., «The evolving EU anti-money laundering regime: Challenges for fundamental rights and the rule of law», *Maastricht Journal of European and Comparative Law*, Vol. 23, 2ª edizione, 2016, pagg. da 261 a 293.

[4](#) V. il preambolo della Carta del Gruppo Egmont delle Unità di informazione finanziaria, approvata nel luglio 2013 dai responsabili delle Unità di informazione finanziaria del Gruppo Egmont.

[5](#) Tale disposizione prevede quanto segue: «[l]’accesso e il trattamento delle informazioni contenute nella banca dati dell’Unità di informazione finanziaria sono riservati a funzionari e dipendenti dell’Unità di informazione finanziaria. Sulla base della presente legge, il direttore

dell'Unità di informazione finanziaria può imporre limitazioni all'accesso alle informazioni, qualificandole come riservate ad uso interno. (...)».

[6](#) Tale disposizione stabilisce quanto segue: «[il] detentore delle informazioni respinge una richiesta di informazioni nei seguenti casi: 1) l'accesso alle informazioni richieste è soggetto a limitazioni e il richiedente non ha diritto di accedere alle informazioni richieste».

[7](#) Direttiva del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione (GU 2015, L 141, pag. 73).

[8](#) Regolamento del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU 2016, L 119, pag. 1) (in prosieguo: il «RGPD»).

[9](#) RT I, 18.12.2020, 38.

[10](#) Direttiva del Parlamento europeo e del Consiglio, del 30 maggio 2018, che modifica la direttiva 2015/849 e che modifica le direttive 2009/138/CE e 2013/36/UE (GU 2018, L 156, pag. 43).

[11](#) Direttiva del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU 2016, L 119, pag. 89).

[12](#) Sentenza del 30 aprile 2024 (C-470/21, EU:C:2024:370, punto 158).

[13](#) Il RGPD prevede una clausola orizzontale all'articolo 23, mentre ai sensi della direttiva 2016/680 ciascun diritto può essere limitato su base individuale. In particolare, per quanto

concerne il diritto di accesso dell'interessato, l'articolo 15 della direttiva 2016/680 consente espressamente agli Stati membri di adottare misure legislative volte a limitare tale diritto, «in tutto o in parte» e ad adottare misure legislative dirette a determinare le «categorie di trattamenti» che possono rientrare, «in tutto o in parte», nelle categorie dei motivi di limitazione. La dottrina giuridica osserva, correttamente, che, sebbene i diritti degli interessati, compreso il diritto di accesso, possano essere limitati anche ai sensi del RGPD, la possibilità di introdurre limitazioni ai sensi della direttiva 2016/680 è più estesa, il che rende più probabile che una persona che chiede accesso ai dati in possesso di un'autorità di contrasto riceva una risposta del tipo «non si conferma e non si smentisce»; v. Mouzakiti, F., «Cooperation between financial intelligence units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive», 2020, Vol. 11, 3^a edizione, *New Journal of European Criminal Law*, pagg. da 351 a 374, in particolare pag. 366.

[14](#) Le decisioni di adeguatezza della Commissione ai sensi dell'articolo 45 del RGPD, volte a stabilire se un paese terzo offra un livello di protezione adeguato, non si applicano agli scambi di dati ai sensi della direttiva 2016/680, per i quali è necessaria una decisione di adeguatezza distinta ai sensi dell'articolo 36 di quest'ultima. In mancanza di siffatta decisione, i trasferimenti possono avvenire in presenza di garanzie adeguate, conformemente all'articolo 37 della direttiva 2016/680.

[15](#) Regolamento del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU 2018, L 295, pag. 39).

[16](#) V. considerando 10 del RGPD.

[17](#) Sentenza del 24 febbraio 2022, *Valsts ienēmumu dienests* (Trattamento di dati personali a fini fiscali) (C-175/20, EU:C:2022:124, punto 40).

[18](#) Sentenza del 24 febbraio 2022, *Valsts ienēmumu dienests* (Trattamento di dati personali a fini fiscali) (C-175/20, EU:C:2022:124, punto 42 e giurisprudenza citata).

[19](#) V. Vogiatzoglou, P., «Scope» in Kosta, E. e Boehm, F. (a cura di), *The EU Law Enforcement Directive (LED)*, Oxford University Press, Oxford, 2024, pagg. da 67 a 77, in particolare pag. 74.

[20](#) Sentenza del 24 febbraio 2022, *Valsts ieņēmumu dienests* (Trattamento di dati personali a fini fiscali) (C-175/20, EU:C:2022:124, punto 43 e giurisprudenza citata).

[21](#) V. considerando 11 della direttiva 2016/680.

[22](#) Sentenza del 24 febbraio 2022, *Valsts ieņēmumu dienests* (Trattamento di dati personali a fini fiscali) (C-175/20, EU:C:2022:124, punto 42 e giurisprudenza citata).

[23](#) V., in tal senso, sentenza del 21 giugno 2022, *Ligue des droits humains* (C-817/19, EU:C:2022:491, punto 67). V. Brewczyńska, M., «A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation» in Kosta, E. *et al.* (a cura di) *Research handbook on EU data protection law*, Edward Elgar, Cheltenham, 2022, pagg. da 91 a 114, in particolare pag. 104.

[24](#) Dall'articolo 23, paragrafo 1, lettere d) e h), del RGPD emerge che i trattamenti di dati personali effettuati da soggetti privati per le finalità di contrasto di cui all'articolo 2, paragrafo 2, lettera d), di tale regolamento rientrano nell'ambito di applicazione di quest'ultimo; v. sentenza del 21 giugno 2022, *Ligue des droits humains* (C-817/19, EU:C:2022:491, punto 68 e giurisprudenza citata).

[25](#) Come risulta dai considerando 11 e 12 della direttiva 2016/680, il RGPD si applica al trattamento dei dati personali che venga effettuato da un'«autorità competente», ai sensi dell'articolo 3, punto 7, di detta direttiva, ma per finalità diverse da quelle di contrasto; sentenza del 24 febbraio 2022, *Valsts ieņēmumu dienests* (Trattamento di dati personali a fini fiscali) (C-175/20, EU:C:2022:124, punto 43 e giurisprudenza citata).

[26](#) La Ceļu satiksmes drošības direkcija (Direzione per la sicurezza stradale, Lettonia).

[27](#) Sentenza del 22 giugno 2021, *Latvijas Republikas Saeima* (Punti di penalità) (C-439/19, EU:C:2021:504, punto 72).

[28](#) Sentenza del 24 febbraio 2022, *Valsts ieņēmumu dienests* (Trattamento di dati personali a fini fiscali) (C-175/20, EU:C:2022:124, punto 44).

[29](#) Direttiva del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi (GU 2016, L 119, pag. 132; in prosieguo: la «direttiva PNR»).

[30](#) Sentenza del 21 giugno 2022, *Ligue des droits humains* (C-817/19, EU:C:2022:491, punto 80).

[31](#) Sentenza del 30 aprile 2024, *La Quadrature du Net e a.* (Dati personali e lotta contro la contraffazione) (C-470/21, EU:C:2024:370, punti 158 e 159).

[32](#) Per una rassegna della genesi delle FIU nel settore AML, v. Parlamento europeo: Servizio Ricerca del Parlamento europeo e Scherrer, A., *Fighting tax crimes – Cooperation between Financial Intelligence Units, Ex-post impact assessment – Study*, marzo 2017, pag. 8 (in prosieguo: lo «studio del Parlamento europeo del 2017»); Mitsilegas, V., «New forms of transnational policing: The emergence of financial intelligence units in the European Union and the challenges for human rights: Part 1», *Journal of Money Laundering Control*, Vol. 3, 2^a edizione, 1999, pag. 147. La cooperazione delle unità specializzate in materia di informazione finanziaria si è concretizzata in occasione del primo «Gruppo Egmont», che si è riunito nel 1995. Nel 2003 il GAFI ha adottato una serie riveduta di 40 raccomandazioni, che includevano formalmente una raccomandazione relativa all'istituzione e al funzionamento delle FIU. Le raccomandazioni del GAFI del 2012, aggiornate nel giugno 2026, contengono una raccomandazione sulle FIU (raccomandazione n. 29).

[33](#) Decisione del Consiglio, del 17 ottobre 2000, concernente le modalità di cooperazione tra le unità di informazione finanziaria degli Stati membri per quanto riguarda lo scambio di informazioni (GU 2000, L 271, pag. 4).

[34](#) Già articolo 34, paragrafo 2, lettera c), TUE.

[35](#) V. Fondo Monetario Internazionale, *Financial Intelligence Units: An Overview*, 2004 (disponibile all'indirizzo:

<https://www.elibrary.imf.org/display/book/9781589063624/9781589063624.xml>), pag. 9. Lo studio del Parlamento europeo del 2017 rinvia, a pagg. 13 e 14, a una relazione del 2016 elaborata dalla piattaforma dell'Unione delle FIU, in cui si fa riferimento a tre modelli di FIU: amministrativo, di contrasto (o giudiziario) e ibrido. I modelli di FIU a cui tale relazione fa riferimento sono distribuiti come segue: 12 FIU dell'Unione hanno natura amministrativa e sono istituite, ad esempio presso il Ministero delle Finanze, il Ministero della Giustizia o il Ministero degli Affari interni, oppure presso la Banca centrale o un'autorità di vigilanza, come accade in Belgio, Bulgaria, Repubblica ceca, Spagna, Francia, Croazia, Italia, Lettonia, Malta, Polonia, Romania e Slovenia; 11 FIU dell'Unione sono organizzate secondo il modello delle autorità di contrasto (di polizia e/o giudiziaria), come in Austria, Estonia, Finlandia, Germania, Irlanda, Lituania, Portogallo, Slovacchia, Svezia, Lussemburgo e Regno Unito; 5 FIU hanno definito la propria natura come «ibrida», in ragione della compresenza di elementi di polizia e amministrativi, come nel caso di Danimarca, Grecia, Cipro, Ungheria e Paesi Bassi. Sulle ragioni che dettano la scelta del modello di FIU, v. Masciandaro, D. e Volpicella, A., «Designing financial supervision: The puzzling case of the FIUs against money laundering», *Journal of Financial Regulation*, volume 2, 1ª edizione, 2016, pagg. da 79 a 113.

36 V. considerando 14 della direttiva (UE) 2019/1153 del Parlamento europeo e del Consiglio, del 20 giugno 2019, che reca disposizioni per agevolare l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati, e che abroga la decisione 2000/642/GAI del Consiglio (GU 2019, L 186, pag. 122).

37 V. articolo 52 della direttiva 2015/849, ai sensi del quale le FIU dovrebbero cooperare tra loro nella misura più ampia possibile, «a prescindere dal loro status organizzativo».

38 V. considerando 14 della direttiva 2019/1153. Tale direttiva, che è stata adottata sulla base dell'articolo 87, paragrafo 2, TFUE, relativo alla cooperazione di polizia, (e che ha abrogato la decisione 2000/642) mirava a rafforzare lo scambio di informazioni finanziarie con le autorità competenti designate, e accrescere la certezza del diritto e l'efficacia operativa. L'articolo 1, paragrafo 2, lettera a), di tale direttiva precisa che essa non pregiudica la direttiva 2015/849 e le relative disposizioni del diritto nazionale, «inclusi lo status organizzativo conferito alle FIU ai sensi del diritto nazionale nonché la loro indipendenza ed autonomia operativa».

39 Gli Stati membri possono affidare alle FIU altri compiti e funzioni, purché non interferiscano con il loro compito principale. Il governo estone ha sostenuto che il RAB svolge anche un ruolo di controllo. Tuttavia, il procedimento principale verte sul diritto di accesso ai dati in possesso della FIU nell'esercizio del suo compito e delle sue funzioni principali.

[40](#) Esse ricevono informazioni dai soggetti obbligati cui si applica la direttiva 2015/849, conformemente al suo articolo 2, paragrafo 1. I soggetti obbligati sono tenuti a informare le FIU, anche mediante la segnalazione di operazioni sospette, a norma dell'articolo 33 di tale direttiva.

[41](#) A tal fine, gli Stati membri devono provvedere, conformemente all'articolo 8 della direttiva 2019/1153, affinché le loro autorità designate competenti siano tenute a rispondere tempestivamente, caso per caso, alle richieste di informazioni in materia di contrasto presentate dalla FIU nazionale, laddove tali informazioni siano necessarie per prevenire, accertare e contrastare il riciclaggio, i reati presupposto associati e il finanziamento del terrorismo.

[42](#) Ciò detto, anche quando le FIU sono integrate in una struttura di polizia o giudiziaria, esse devono mantenere la propria indipendenza e autonomia operativa. V. articolo 19, paragrafo 4, della direttiva (UE) 2024/1640 del Parlamento europeo e del Consiglio, del 31 maggio 2024, relativa ai meccanismi che gli Stati membri devono istituire per prevenire l'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica la direttiva (UE) 2019/1937, e modifica e abroga la direttiva 2015/849 (con effetto a decorrere dal 10 luglio 2027) (GU L, 2024/1640) (sesta direttiva antiriciclaggio).

[43](#) Mouzakiti, F., nota 13, op. cit., pag. 373, che descrive le FIU come istituzioni di «nuova polizia» [traduzione libera].

[44](#) Il Regno dei Paesi Bassi, nelle sue osservazioni orali, ha evitato di prendere posizione sulla questione della disciplina applicabile alle FIU in materia di protezione dei dati.

[45](#) Su tale base, la direttiva (UE) 2018/1673 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla lotta al riciclaggio mediante il diritto penale (GU 2018, L 284, pag. 22), stabilisce requisiti relativi alla configurazione del riciclaggio come reato.

[46](#) Ciò è sottolineato anche dal Consiglio d'Europa: comitato di esperti per la valutazione delle misure antiriciclaggio e del finanziamento del terrorismo. (Moneyval) nella presentazione delle funzioni delle FIU (disponibile all'indirizzo: <https://www.coe.int/en/web/moneyval/implementation/fiu>). Secondo l'associazione Transparency International, quando le FIU analizzano informazioni, esse «riuniscono informazioni frammentarie che nessuna singola banca o autorità potrebbe cogliere nella loro interezza» [traduzione libera] (v. <https://www.transparency.org/en/news/financial-intelligence-units-powerful-tools-against-corruption>).

[47](#) Mouzakiti, F., nota 13, op. cit., pag. 353 [traduzione libera].

[48](#) V. Senato francese, «*Rapport fait au nom de la commission d'enquête aux fins d'évaluer les outils de la lutte contre la délinquance financière, la criminalité organisée et le contournement des sanctions internationales, en France et en Europe, et de proposer des mesures face aux nouveaux défis*», Vol. I, 18 giugno 2005, pag. 197, [traduzione libera], in cui si sottolinea che la FUI francese (Tracfin) si colloca al confine tra attività di prevenzione e perseguimento dei reati («à la frontière entre les volets préventif et répressif»).

[49](#) Sentenza del 30 aprile 2024 (C-470/21, EU:C:2024:370).

[50](#) Paragrafo 42 delle presenti conclusioni.

[51](#) Sentenza del 30 aprile 2024, La Quadrature du Net e a. (Dati personali e lotta contro la contraffazione) (C-470/21, EU:C:2024:370, punto 158).

[52](#) *Ibidem*.

[53](#) V. paragrafo 41 delle presenti conclusioni.

[54](#) Sentenza del 21 giugno 2022 (C-817/19, EU:C:2022:491, punti 79 e 80).

[55](#) V. paragrafo 36 delle presenti conclusioni.

[56](#) V. paragrafo 43 delle presenti conclusioni.

[57](#) Per completezza rilevo che, come risulta dal considerando 14 della direttiva 2016/680, quest'ultima non si applica al trattamento di dati nel contesto di un'attività che non rientra nell'ambito di applicazione del diritto dell'Unione, in particolare le attività concernenti la sicurezza nazionale.

[58](#) Tale conclusione è corroborata dalla sentenza del 21 giugno 2022, *Ligue des droits humains* (C-817/19, EU:C:2022:491), in cui la Corte ha dichiarato che le UIP devono essere classificate come «autorità competenti» ai sensi della direttiva 2016/680. Siffatta classificazione non era esclusa dal fatto che le UIP trasferissero dati PNR o il risultato di un trattamento alle autorità competenti.

[59](#) Ad esclusione del governo dei Paesi Bassi, che non ha preso posizione su tale questione.

[60](#) Decisione quadro del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (GU 2008, L 350, pag. 60).

[61](#) V. articolo 19, paragrafo 4, secondo comma, della direttiva 2024/1640.

[62](#) In particolare, consentire al soggetto obbligato o all'autorità nazionale competente di svolgere adeguatamente i suoi compiti e non compromettere indagini, analisi, inchieste o procedimenti ufficiali o giudiziari ai fini di tale direttiva e garantire che non sia compromessa la prevenzione, l'indagine e l'individuazione del riciclaggio e del finanziamento del terrorismo. L'esistenza di una siffatta limitazione settoriale specifica del diritto di accesso dell'interessato, con riguardo al divieto di comunicazione, può forse essere spiegata dal fatto che la direttiva 2015/849 è anteriore all'adozione dello strumento dell'Unione in materia di protezione dei dati nel settore delle attività di contrasto, vale a dire la direttiva 2016/680. La direttiva 2024/1640, che, come menzionato in precedenza (paragrafo 81 delle presenti conclusioni), abroga la direttiva 2015/849, non contiene più tale disposizione relativa alla limitazione del diritto di accesso.

[63](#) Oppure a un organo di autoregolamentazione della professione, conformemente alle condizioni di cui all'articolo 34 della direttiva 2015/849.

[64](#) V. paragrafo 60 delle presenti conclusioni.

[65](#) Qualora la Corte ritenga che l'articolo 41, paragrafo 4, della direttiva 2015/849 sia applicabile a tutti i dati in possesso delle FIU, la mia analisi relativa alla quarta questione resta

rilevante, in quanto tale disposizione riflette, in sostanza, le principali condizioni per la limitazione del diritto di accesso previste all'articolo 15, paragrafo 1, della direttiva 2016/680.

[66](#) V. Dimitrova, D., «Limitations to the right of access» in Kosta, E. e Boehm, F. (a cura di), nota 19, op. cit., pag. 288.

[67](#) Sentenza del 6 ottobre 2020, Privacy International (C-623/17, EU:C:2020:790, punto 64).

[68](#) V. articolo 38, paragrafo 2, e articolo 42 della direttiva 2015/849, e articolo 61, paragrafo 3, terzo comma, della medesima.

[69](#) Sentenza del 22 novembre 2022, Luxembourg Business Registers (C-37/20 e C-601/20, EU:C:2022:912, punto 63).

[70](#) Sentenza del 22 novembre 2022, Luxembourg Business Registers (C-37/20 e C-601/20, EU:C:2022:912, punto 64).

[71](#) Sentenza del 18 giugno 2026, NTH Haustechnik (C-484/24, EU:C:2026:496, punto 72 e giurisprudenza citata).

[72](#) Sentenza del 6 ottobre 2020, Privacy International (C-623/17, EU:C:2020:790, punto 68 e giurisprudenza citata).

[73](#) V. Dimitrova, D., nota 66, op. cit., pag. 292, che sottolinea che l'obbligo di documentazione mira a garantire che non siano imposte limitazioni arbitrarie.

[74](#) Siffatte garanzie dovrebbero fare salve le garanzie previste dal diritto penale nazionale nel caso in cui l'interessato sia formalmente accusato di un reato.

[75](#) Sentenza del 16 novembre 2023 (C-333/22, EU:C:2023:874, punto 44).

[76](#) *Ibidem*, punto 66.

[77](#) *Ibidem*, punto 69 e giurisprudenza citata.

[78](#) *Ibidem*, punto 70.

[79](#) Sentenza del 16 luglio 2026, AEDT e État du Grand-Duché de Luxembourg (C-158/25, EU:C:2026:591, punto 21).

[80](#) V. paragrafi 88 e ss. delle presenti conclusioni.

[81](#) Sentenza del 16 novembre 2023, Ligue des droits humains (Verifica del trattamento dei dati da parte dell'autorità di controllo), (C-333/22, EU:C:2023:874, punto 42).

[82](#) V. paragrafo 109 delle presenti conclusioni.

[83](#) V. paragrafo 102 delle presenti conclusioni.

[84](#) Sentenza del 18 giugno 2026, NTH Haustechnik (C-484/24, EU:C:2026:496, punto 71 e giurisprudenza citata).

[85](#) *Ibidem*, punto 72 e giurisprudenza citata.

[86](#) *Ibidem*, punto 74 e giurisprudenza citata.

[87](#) Corte EDU, 23 gennaio 2025, H.W. c. Francia, CE:ECHR:2025:0123JUD001380521, § 65 e giurisprudenza citata.

[88](#) V., in tal senso, sentenza del 18 giugno 2026, NTH Haustechnik (C-484/24, EU:C:2026:496, punto 75, che cita, in tal senso, Corte EDU, 23 gennaio 2025, H.W. c. Francia, CE:ECHR:2025:0123JUD001380521, § 65 e giurisprudenza citata).

[89](#) V., in tal senso, sentenza del 24 febbraio 2022, Valsts ieņēmumu dienests (Trattamento di dati personali a fini fiscali) (C-175/20, EU:C:2022:124, punto 56).

[90](#) V. paragrafi 100 e ss. delle presenti conclusioni.

[91](#) Articoli da 8 a 17 dello statuto della banca dati del RAB.

[92](#) Il livello di sicurezza dei dati trattati è definito «elevato» all'articolo 5, paragrafo 2, dello statuto della banca dati del RAB.

[93](#) L'articolo 26, paragrafo 1, dello statuto della banca dati del RAB precisa che i dati contenuti nella banca dati e i documenti riguardanti una persona ivi inseriti sono conservati per 15 anni dopo la chiusura della rispettiva segnalazione o pratica. I dati relativi a una persona, i collegamenti di tale persona con altri dati e i documenti relativi alla persona sono cancellati dalla banca dati in modo da garantire l'integrità dei dati relativi alle persone, alle segnalazioni e alle pratiche.

[94](#) V. paragrafo 107 delle presenti conclusioni.