Causa C-60/22

Sintesi della domanda di pronuncia pregiudiziale ai sensi dell'articolo 98, paragrafo 1, del regolamento di procedura della Corte di giustizia

Data di deposito:

1° febbraio 2022

Giudice del rinvio:

Verwaltungsgericht Wiesbaden (Tribunale amministrativo, Wiesbaden, Germania)

Data della decisione di rinvio:

27 gennaio 2022

Ricorrente:

UZ

Resistente:

Repubblica federale di Germania

Oggetto del procedimento principale

Normativa in materia di protezione dei dati personali – Regolamento 2016/679 (regolamento generale sulla protezione dei dati) – Articolo 5, paragrafo 2 – Responsabilizzazione – Articoli 17, paragrafo 1, lettera d), e 18, paragrafo 1, lettera b) – Liceità del trattamento – Diritto alla cancellazione o diritto di limitazione del trattamento – Utilizzo dei dati trattati

Oggetto e fondamento giuridico del rinvio

Interpretazione del diritto dell'Unione, articolo 267 TFUE

Questioni pregiudiziali

1) Se l'omissione o l'assente o incompleta applicazione, da parte del titolare del trattamento, del principio di responsabilizzazione ai sensi dell'articolo 5 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, RGPD), per esempio per l'omessa o incompleta tenuta di un registro delle attività di trattamento ai sensi dell'articolo 30 del RGPD, o per la mancata determinazione di una procedura per la contitolarità ai sensi dell'articolo 26 del RGPD, comportino un trattamento illecito dei dati personali ai sensi degli articoli 17, paragrafo 1, lettera d), e 18, paragrafo 1, lettera b), del RGPD, cosicché sussiste per l'interessato un diritto alla cancellazione o un diritto di limitazione di trattamento.

2) In caso di risposta affermativa alla prima questione: se la sussistenza di un diritto alla cancellazione o di un diritto di limitazione di trattamento comporti che i dati trattati non possano essere presi in considerazione nell'ambito di un procedimento giudiziario. Se ciò si applichi in ogni caso qualora l'interessato si opponga all'utilizzo in sede giudiziale.

3) In caso di risposta negativa alla prima questione: se una violazione da parte di un titolare del trattamento degli articoli 5, 30 o 26 del RGPD comporti, in merito alla questione dell'utilizzo in sede giudiziale del trattamento dei dati personali, che un giudice nazionale possa tener conto dei dati solo se l'interessato presta espressamente il suo consenso.

Disposizioni di diritto dell'Unione richiamate

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; in prosieguo: il «RGPD») (GU 2016, L 119, pag. 1), considerando 82, articoli 5, 9, 17, 18, 26, 30, 94

Direttiva 2013/32/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, recante procedure comuni ai fini del riconoscimento e della revoca dello status di protezione internazionale (GU 2013, L 180, pag. 60), considerando 52

Carta dei diritti fondamentali dell'Unione europea, articoli 7 e 8

Disposizioni nazionali richiamate

Bundesdatenschutzgesetz (legge federale sulla protezione dei dati; in prosieguo: il «BDSG») (BGBl. I, pag. 2097), articolo 43, paragrafo 3

Breve illustrazione dei fatti e del procedimento

1 Il ricorrente contesta la decisione di diniego del Bundesamt für Migration und Flüchtlinge (Ufficio federale per l'immigrazione e i rifugiati) e chiede il riconoscimento dello status di rifugiato ai sensi dell'articolo 3 dell'Asylgesetz (legge in materia di asilo; in prosieguo: l'«AsylG»). La decisione dell'Ufficio resistente si fonda sul cosiddetto fascicolo elettronico MARIS, che viene trasmesso al giudice alla casella postale elettronica giudiziaria e amministrativa (EGVP) anche nel quadro di una procedura di contitolarità ai sensi dell'articolo 26 [del RGPD]. Per quanto riguarda le questioni relative alla completa trasmissione degli atti, si fa riferimento alle questioni già sottoposte alla Corte di giustizia (causa C-564/21).

2 Non è certo che, presso l'Ufficio resistente, in generale esista o venga tenuto in modo completo un registro delle attività di trattamento ai sensi dell'articolo 30 del RGPD in relazione al cosiddetto fascicolo elettronico MARIS. Non esistono neppure accordi o norme di diritto ai sensi dell'articolo 26 del RGPD riguardo alla procedura per la trasmissione elettronica del fascicolo e alla determinazione delle responsabilità nell'ambito di tale procedura. Tali documenti sono stati richiesti dal giudice del rinvio nel corso del procedimento. L'Ufficio resistente ha tuttavia negato la loro presentazione adducendo la motivazione che non sussisterebbe un accordo ai sensi dell'articolo 26 del RGPD riguardo all'EGVP.

Breve illustrazione della motivazione del rinvio pregiudiziale

3 Il giudice a quo solleva la questione, perlomeno nell'ipotesi che vi sia una (formale) illiceità del trattamento di dati personali del ricorrente da parte dell'Ufficio resistente, relativa al comportamento da assumere in relazione a tali dati, visto che, in conformità della direttiva 2013/32, l'RGPD si applica alle procedure di asilo ai sensi del diritto nazionale. Né l'AsylG né la Verwaltungsgerichtsordnung (codice di procedura dei tribunali amministrativi) contengono precisazioni in tal senso.

4 Ai sensi del considerando 52 della direttiva 2013/32, la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, disciplina il trattamento dei dati personali effettuato negli Stati membri a norma della direttiva medesima. La direttiva 95/46 è stata abrogata, ai sensi dell'articolo 95, paragrafo 1, del RGPD, a decorrere dal 25 maggio 2018. Tuttavia, in conformità dell'articolo 94, paragrafo 2, del RGPD, i riferimenti alla direttiva 95/46 abrogata si intendono fatti a tale regolamento. Il RGPD trova pertanto piena applicazione alle procedure ai fini del riconoscimento dello status di protezione internazionale.

5 Già la direttiva 95/46 prevedeva una documentazione dei trattamenti automatizzati, la cosiddetta notificazione ai sensi dell'articolo 18 di tale direttiva. L'oggetto della notificazione di cui all'articolo 19 della direttiva 95/46

corrispondeva in sostanza all'odierno articolo 30 del RGPD, laddove la nuova disposizione si riferisce a tutte le forme di trattamento, compresi quindi anche gli archivi di dati personali.

6 Nel corso del periodo di vigenza della direttiva 95/46, l'Ufficio resistente disponeva solo di un rudimentale registro dei trattamenti quale notificazione ai sensi della direttiva 95/46 (articolo 4e del BDSG nella vecchia versione) con riferimento ai fascicoli elettronici MARIS. Il registro dei trattamenti dell'epoca (la notificazione) non prevedeva norme specifiche per il trattamento di categorie particolari di dati personali ai sensi dell'articolo 9 del RGPD (articolo 8 della direttiva 95/46). Tali norme specifiche per il trattamento di dati personali ai sensi degli articoli 9 e 10 del RGPD non sembrano esistere neppure oggi. Infatti i dati relativi alla salute e alla religione, così come le condanne penali, sono inseriti in generale nel fascicolo elettronico MARIS come cosiddetti «documenti normali». Non si ravvisa una particolare protezione della sicurezza dei dati, a parte che senz'altro vengono protocollati gli accessi. Comunque il fascicolo di un richiedente asilo può essere consultato da qualsiasi sito esterno dell'Ufficio resistente in tutta la Germania allo stesso modo che dalla sede centrale.

7 Proprio riguardo alla gestione dei fascicoli e alla presentazione degli atti all'organo giurisdizionale, il giudice del rinvio nutre notevoli dubbi sul fatto che l'Ufficio resistente si attenga ai requisiti di cui all'articolo 5, paragrafo 1, del RGPD, in combinato disposto con gli articoli 26 e 30 del medesimo regolamento. Contrariamente a quanto richiesto dal giudice, il registro delle attività di trattamento non è stato presentato. In tal senso è prevista, dopo la pronuncia della Corte di giustizia, un'audizione del direttore dell'organismo titolare del trattamento, vale a dire dell'Ufficio resistente, in relazione alla sua responsabilizzazione ai sensi dell'articolo 5, paragrafo 2, del RGPD.

8 Prima di un'audizione occorre tuttavia chiarire se il mancato adempimento di obblighi previsti dal RGPD e la conseguente illiceità del trattamento di dati personali comporti una sanzione, quale la cancellazione dei dati ai sensi dell'articolo 17, paragrafo 1, lettera d), del RGPD o una limitazione di trattamento ai sensi dell'articolo 18, paragrafo 1, lettera b), del regolamento medesimo. Ciò perlomeno nei casi in cui lo richieda l'interessato, nella specie il ricorrente. Infatti, diversamente, il giudice sarebbe costretto, nell'ambito del procedimento giurisdizionale, a partecipare a un trattamento dei dati personali illecito. L'autorità potrebbe continuare a violare il RGPD senza incorrere in sanzioni.

9 In un caso del genere potrebbe intervenire solo l'autorità di controllo ai sensi dell'articolo 58 del RGPD. Tuttavia, il diritto nazionale non prevede l'irrogazione di sanzioni amministrative pecuniarie al Bundesamt für Migration und Flüchtlinge. Ai sensi dell'articolo 43, paragrafo 3, del BDSG, che si fonda sull'articolo 83, paragrafo 7, del RGPD, non vengono inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici. L'autorità non sarebbe incentivata a comportarsi in maniera lecita. Ciò avrebbe come

conseguenza una scarsa osservanza delle prescrizioni della direttiva 2013/32, così come dello stesso RGPD.

10 La Corte ha già dichiarato che, al momento della realizzazione di un trattamento, occorre che si sia provveduto alla completa «notificazione» (oggi; il registro delle attività di trattamento), ma non prima (cause C-92/09 e 93/09, sentenza del 9 novembre 2011, ECLI:EU:C:2010:662, punti 95 e segg.). Nella specie i dati personali del ricorrente sono stati trattati dall'Ufficio resistente fin dal momento in cui aveva presentato la domanda di asilo (il 7 maggio 2019) Perciò in quel momento, perlomeno secondo la giurisprudenza della Corte, doveva essere tenuto un registro completo delle attività di trattamento con riferimento al fascicolo MARIS (e quindi alla procedura di asilo del ricorrente). Tuttavia, non è questo il caso.

11 La Corte non ha definito le norme applicabili nella specie, né ai sensi della direttiva 95/46, né sulla base del RGPD. Se si muove dal presupposto che il titolare del trattamento o il responsabile del trattamento, per dimostrare che si conforma al RGPD, debba tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità (considerando 82 del RGPD), sorge la questione relativa alle conseguenze che derivano dall'omissione dell'organo responsabile. Infatti in quel caso non è possibile rispettare il principio di responsabilizzazione ai sensi dell'articolo 5 del RGPD.

12 È vero che l'articolo 83, paragrafo 5, lettera a), del RGPD stabilisce che una violazione del principio di responsabilizzazione di cui all'articolo 5 del RGPD è soggetta a sanzioni amministrative pecuniarie fino a EUR 20 000 000. Tuttavia, come già illustrato, ai sensi dell'articolo 43, paragrafo 3, del BSDG, ciò non si applica ad autorità pubbliche federali. Ad ogni modo, l'articolo 17, paragrafo 1, lettera d), del RGPD stabilisce che i dati personali trattati illecitamente devono essere cancellati, perlomeno su richiesta dell'interessato.

13 Sulla base dell'omessa o incompleta tenuta di un registro delle attività di trattamento, il giudice del rinvio è giunto alla conclusione, quantomeno alla luce dell'articolo 5 del RGPD, che sotto il profilo «formale» sussista un trattamento dei dati personali illecito. Sorge pertanto la questione di stabilire se in un caso del genere non si debba procedere, quale sanzione per un'omissione ai sensi dell'articolo 5 del RGPD in combinato disposto con l'articolo 30 del regolamento medesimo, alla cancellazione o almeno al congelamento dei dati personali. Infatti, in caso contrario, in mancanza di una possibile sanzione, non si potrebbe realizzare un'attuazione efficace del RGPD.

14 Perlomeno, a quanto consta, la Repubblica francese aveva stabilito a livello di diritto nazionale, per esempio, nel corso del periodo di vigenza degli articoli 18 e segg. della direttiva 95/46, che nell'ambito di procedimenti giurisdizionali vigesse per legge un divieto tassativo di utilizzo per i dati personali non compresi in una notificazione da parte dell'organismo titolare del trattamento all'autorità di controllo (CNIL), in quanto l'utilizzo dei dati in assenza di documentazione

risultava illecito. Con ciò, in tal caso, veniva già applicata una sanzione per il fatto che i dati personali non potevano essere trattati e utilizzati dal giudice. In vigenza del RGPD, anche in Portogallo e in altri Stati membri è previsto che la mancanza di un registro delle attività di trattamento determini un divieto di utilizzo. Un meccanismo a cui non si è fatto ricorso nella Repubblica federale di Germania in sede di attuazione della direttiva 95/46 e neppure durante la vigenza del RGPD. Qui, piuttosto, si sono gettate le basi per una «tolleranza» dell'assenza di notificazione.

15 Anche la trasmissione elettronica dei fascicoli e degli atti dell'Ufficio resistente costituisce un trattamento di dati personali ai sensi dell'articolo 4, punto 2, del RGPD, per il quale occorre osservare i principi applicabili al trattamento di dati personali di cui all'articolo 5 di detto regolamento. Pertanto, anche a tale riguardo, sorgono dubbi su una liceità formale del trattamento di dati personali che avviene con l'invio del cosiddetto fascicolo elettronico e degli atti dell'Ufficio resistente attraverso i rispettivi canali di trasmissione. In questo caso, parimenti, manca un registro delle attività di trattamento e un accordo sulla contitolarità del trattamento. In realtà esiste la Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (normativa concernente le condizioni tecniche quadro per la giustizia elettronica e le caselle speciali di posta elettronica delle autorità) del 24 novembre 2017 (BGBl. I, pag. 3803, come modificata dall'articolo 6 della legge del 5 ottobre 2021, BGBl. I, pag. 4607) che disciplina la trasmissione di documenti elettronici ai giudici a livello dei Land (Stati federati) e del Bund (lo Stato federale). In tale contesto le massime autorità dello Stato federale o dei governi degli Stati federati possono verificare, per il loro settore nell'ambito degli enti di diritto pubblico, l'identità delle autorità o delle persone giuridiche di diritto pubblico al fine di autorizzarne l'accesso al sistema delle caselle speciali di posta elettronica delle autorità (cosiddetto BeBPo). Le massime autorità dello Stato federale o diversi governi degli Stati federati possono anche individuare un ente di diritto pubblico comune per i loro settori. Non è definito chi sia di fatto tale ente. In definitiva, in tale ambito si colloca senz'altro il cosiddetto gruppo di lavoro dei ministeri della Giustizia dello Stato federale e degli Stati federati [commissione Stato federale - Stati federati per le tecnologie dell'informazione nel settore della giustizia (BLK), gruppo di lavoro norme informatiche nel settore della giustizia]. Non è noto e non è documentato quali siano la/le autorità responsabili della tenuta di registri relativi alle caselle elettroniche EGVP o BeBPo o persino della necessaria struttura server.

16 Inoltre non esistono disposizioni di legge adeguate o altre norme scritte che disciplinino le responsabilità tra giudici e autorità, come sarebbe richiesto dall'articolo 26 del RGPD. Anche negli Stati federati che hanno scelto in base al loro statuto il modello di contitolarità, manca una corrispondente attuazione conforme alla protezione dei dati. In Assia lo statuto stabilisce addirittura che la casella elettronica sia collegata esclusivamente ai server del «centro elaborazione dati» del settore della giustizia, vale a dire presso la centrale per l'elaborazione dati dell'Assia (HZD). In tale situazione, l'HZD non fa comunque parte del settore

della giustizia e tuttalpiù, quale intermediario, è un responsabile del trattamento ai sensi dell'articolo 28 del RGPD.

17 È noto solo che di fatto il Landesamt für Datensicherheit in Nordrhein-Westfalen (ufficio del Land per la sicurezza dei dati nella Renania settentrionale-Vestfalia), in qualità di «intermediario», dovrebbe essere competente per l'amministrazione e il funzionamento del server del registro di sistema S.A.F.E. centrale comune ai diversi Stati federati. L'ID SAFE dev'essere non modificabile e può essere assegnato una sola volta (v., in proposito, SAFE – http://www.egvp.de/Drittprodukte/SAFE_Abbildungsvorschrift _SAFE_ID_Stand_Dez_2014.pdf). Inoltre le caselle postali nel sistema EGVP sono contrassegnate con un numero identificativo univoco (cosiddetto ID Govello). A quanto consta al giudice del rinvio, tali ID devono essere riportati in un registro a cura del servizio informatico della Renania settentrionale-Vestfalia (IT-NRW). Non è stabilito chi sia effettivamente responsabile dell'attribuzione dell'ID Govello nell'ambito della rete creata tra Stato federale e Stati federati.

18 Non è noto su quale fondamento giuridico per la protezione dei dati si basi il sistema EGVP. In merito alla questione di un accordo ai sensi dell'articolo 26 del RGPD, l'Ufficio resistente si è rifiutato di esprimersi e di presentare detto accordo. In tal senso appare dubbio altresì se sia possibile effettuare una trasmissione lecita attraverso le cosiddette caselle speciali di posta elettronica senza che siano state definite le responsabilità ai sensi dell'articolo 26 del RGPD. Ciò anche con riguardo alla sicurezza dei dati, poiché nessuno dei documenti in tale canale di trasmissione è cifrato.

19 Secondo il parere del giudice del rinvio, non è determinante stabilire se, in base all'attuale diritto positivo, occorra utilizzare una crittografia end-to-end per le caselle speciali di posta elettronica degli avvocati. Non esiste, perlomeno in Assia, alcuna crittografia dei messaggi scambiati tra l'intermediario, l'HZD, e il rispettivo tribunale, compreso quindi il Verwaltungsgericht Wiesbaden (Tribunale amministrativo di Wiesbaden, Germania).

20 Non è tuttavia questo l'oggetto della discussione, in quanto la procedura applicata equivale a un sistema di posta elettronica. In merito al servizio di posta elettronica su Internet Gmail, la Corte di giustizia ha dichiarato che non si tratta di un servizio di comunicazione elettronica, in quanto tale servizio, non comprendendo la fornitura di un accesso a Internet, non consiste interamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica e non costituisce pertanto un «servizio di comunicazione elettronica» (sentenza del 13 giugno 2019, C-193/18, ECLI:EU:C:2019:498). Quindi, l'EGVP non costituisce un servizio che ricade nell'ambito di applicazione della direttiva 2002/58/CE (articolo 2, paragrafo 4, del RGPD). Pertanto il RGPD è applicabile, con la conseguenza che l'EGVP e le procedure ad esso connesse devono essere riportati in un registro delle attività di trattamento, concordando le rispettive responsabilità con molti titolari del trattamento ai sensi dell'articolo 26 del RGPD. Nella specie mancano

entrambe le cose. Per questo motivo sussistono dubbi sulla liceità del trattamento di dati personali.

21 Il sistema EGVP riguarda procedure nell'ambito delle amministrazioni della giustizia, da coordinare con il secondo potere, l'esecutivo, e l'Ufficio resistente, che fa anch'esso parte del potere esecutivo. In tal senso l'Ufficio resistente deve provvedere, secondo il giudice del rinvio, affinché la procedura elettronica di trasmissione dei dati personali e degli atti sia conforme al RGPD.

22 Il giudice del rinvio ritiene che, nell'ambito delle attività nel settore della giustizia, si ponga la questione di stabilire come trattare i dati personali forniti attraverso il sistema EGVP per mezzo delle cosiddette caselle di posta elettronica delle autorità, se la procedura di EGVP e il trattamento di dati personali connesso in quanto tali non sono conformi al RGPD.

23 Il giudice del rinvio è tenuto ad osservare e ad applicare il RGPD nell'ambito delle sue funzioni giurisdizionali.

24 Esso non ha alcuna influenza sulla liceità del trattamento di dati personali nel settore dell'amministrazione della giustizia, in quanto tale trattamento si svolge al di fuori dei «compiti giurisdizionali», a livello di secondo potere, l'esecutivo. Il giudice del rinvio è tuttavia tenuto a osservare e rispettare il diritto dell'Unione. Quando una delle parti nel procedimento viola tali disposizioni, senz'altro non dovrebbe essere consentito un utilizzo dei dati in sede giudiziale, in quanto, in caso contrario, il giudice sarebbe coinvolto in un trattamento di dati personali illecito. Nella specie si deve aggiungere l'aggravante che l'Ufficio resistente, alla luce della corrispondenza fin qui scambiata, certamente viola (consapevolmente) le prescrizioni di diritto dell'Unione.

25 Del resto non si tratta di una fattispecie che giustificherebbe un utilizzo [dei dati] da parte dell'Ufficio resistente ai sensi dell'articolo 17, paragrafo 3, lettera e), del RGPD per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. I dati personali servono effettivamente all'Ufficio resistente per l'adempimento di un obbligo legale che richiede il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, articolo 17, paragrafo 3, lettera b), del RGPD. Tuttavia, in tal modo verrebbe nel contempo legalizzato, a lungo termine, un comportamento illecito in materia di trattamento di dati personali.

26 Per questi motivi le questioni pregiudiziali sottoposte rivestono particolare importanza ai fini dell'attuazione del RGPD nell'ambito del procedimento giurisdizionale. Vi è il rischio di inficiare la finalità di cui all'articolo 1, paragrafo 2, del RGPD di promuovere i diritti e le libertà fondamentali delle persone fisiche, in particolare il loro diritto alla protezione dei dati personali.

27 In tal senso, almeno in caso di risposta negativa alla prima questione, occorrerebbe una disposizione dell'interessato, o meglio l'esplicito consenso

dell'interessato – nella specie il ricorrente – affinché i suoi dati personali possano essere utilizzati nell'ambito di un procedimento giudiziario, nonostante un trattamento formalmente illecito.

28 Ciò avrebbe comunque la conseguenza che, in caso di rifiuto, i dati personali trattati dall'Ufficio resistente, che esso presenta sotto forma del cosiddetto fascicolo elettronico MARIS, non possano essere trattati (utilizzati) dal giudice. Ne deriverebbe altresì che, fino a quando siano soddisfatti gli obblighi di documentazione, verrebbe a mancare un fondamento per la decisione. La decisione originaria dell'Ufficio resistente dovrebbe in ogni caso essere annullata. Fino a quando non siano soddisfatti gli obblighi di documentazione non è possibile adottare una decisione sul riconoscimento del diritto di asilo.