

Causa C-61/22**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 di Wiesbaden, Germania)

Data della decisione di rinvio:

13 gennaio 2022

Ricorrente:

RL

Resistente:

Landeshauptstadt Wiesbaden

Oggetto del procedimento principale

Inserimento e memorizzazione delle impronte digitali nelle carte d'identità – Articolo 3, paragrafo 5, del regolamento (UE) 2019/1157 – Validità – Procedura di adozione del regolamento – Articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea – Articolo 35, paragrafo 10, del regolamento generale sulla protezione dei dati

Oggetto e fondamento giuridico del rinvio pregiudiziale

Validità dell'articolo 3, paragrafo 5, del regolamento (UE) 2019/1157, articolo 267 TFUE

Questione pregiudiziale

Se l'obbligo di inserire e memorizzare le impronte digitali nelle carte d'identità in forza dell'articolo 3, paragrafo 5, del regolamento (UE) 2019/1157 del Parlamento

europeo e del Consiglio, del 20 giugno 2019, sul rafforzamento della sicurezza delle carte d'identità dei cittadini dell'Unione e dei titoli di soggiorno rilasciati ai cittadini dell'Unione e ai loro familiari che esercitano il diritto di libera circolazione (GU L 188 del 12 luglio 2019, pag. 67), costituisca una violazione del diritto dell'Unione di rango superiore, in particolare

- a) dell'articolo 77, paragrafo 3 TFUE
- b) degli articoli 7 e 8 della Carta dei diritti fondamentali
- c) dell'articolo 35, paragrafo 10, del regolamento generale sulla protezione dei dati

e sia quindi invalido per uno di tali motivi.

Disposizioni pertinenti di diritto dell'Unione

Carta dei diritti fondamentali dell'Unione europea: articoli 7, 8, 52;

Trattato sul funzionamento dell'Unione europea: articoli 21, 77, 289;

Regolamento (UE) 2019/1157 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sul rafforzamento della sicurezza delle carte d'identità dei cittadini dell'Unione e dei titoli di soggiorno rilasciati ai cittadini dell'Unione e ai loro familiari che esercitano il diritto di libera circolazione: considerando 2, 17, 18, 19, 21, 22, 40, 41, articoli 3, 11;

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): articoli 9, 35.

Disposizioni nazionali pertinenti

Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz) (legge relativa alle carte di identità e all'identificazione elettronica – legge sulle carte di identità; in prosieguo: il «PAuswG»): articoli 5, 9.

Breve esposizione dei fatti e del procedimento

- 1 Il ricorrente chiede il rilascio di una carta d'identità senza l'inserimento delle impronte digitali. La resistente vi oppone un rifiuto, in quanto l'articolo 5, paragrafo 9, del PAuswG, che trova il suo fondamento nel regolamento (UE) 2019/1157, prevede l'inserimento obbligatorio di due impronte digitali.

- 2 Il regolamento (UE) 2019/1157 è entrato in vigore il 2 agosto 2021. L'articolo 3, paragrafo 5, di detto regolamento stabilisce che le carte d'identità rilasciate dagli Stati membri hanno un supporto di memorizzazione contenente un'immagine del volto del titolare e due impronte digitali in formato interoperativo digitale. Anche la normativa tedesca contiene disposizioni concernenti l'inserimento delle impronte digitali nelle carte d'identità (articolo 5, paragrafo 9, del PAuswG), ritenendo il legislatore tedesco, come risulta dalla relazione illustrativa, che le impronte digitali dovessero essere inserite in forza dell'articolo 3, paragrafo 5, del regolamento menzionato.
- 3 In data 30 novembre 2021, il ricorrente chiedeva il rilascio di una nuova carta d'identità senza impronte digitali a causa del malfunzionamento del chip della sua precedente carta d'identità. Il nuovo rilascio veniva rifiutato in ragione dell'asserita obbligatorietà dell'inserimento delle impronte digitali a decorrere dal 2 agosto 2021. Inoltre, il ricorrente non avrebbe alcun diritto al rilascio di una nuova carta d'identità, essendo già in possesso di un valido documento d'identità. La carta d'identità resterebbe valida anche con un chip difettoso.
- 4 L'autorità competente per il rilascio delle carte d'identità in base alla normativa tedesca opera in qualità di autorità di prevenzione dei rischi. Nondimeno, il rilascio delle carte d'identità e il correlato trattamento dei dati non sono soggetti alla direttiva (UE) 2016/680, bensì, come può evincersi dal considerando 40 del regolamento (UE) 2019/1157, al regolamento generale sulla protezione dei dati (in prosieguo: il «RGPD»). Nella fattispecie in esame, il sindaco non opera pertanto nel settore del diritto dell'Unione in materia di prevenzione dei rischi, che deve essere interpretato in modo autonomo. Ai sensi dell'articolo 1, paragrafo 1, e dell'articolo 2, paragrafo 1, della suddetta direttiva, essa si applica solo quando le autorità pubbliche operano 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, in cui non rientra il settore dei passaporti e delle carte d'identità.

Breve esposizione della motivazione del rinvio pregiudiziale

- 5 La decisione della questione pregiudiziale è necessaria ai fini della sentenza. Ove l'articolo 3, paragrafo 5, del regolamento (UE) 2019/1157 violi il diritto dell'Unione europea di rango superiore, il ricorrente ha diritto al rilascio di una carta d'identità senza l'inserimento delle impronte digitali, ai sensi dell'articolo 9, paragrafo 1, prima frase, del PAuswG. La normativa nazionale dell'articolo 5, paragrafo 9, del PAuswG perderebbe il proprio fondamento a causa della violazione del diritto dell'Unione.
- 6 Pur essendo la precedente carta d'identità del ricorrente ancora valida nonostante il chip difettoso ai sensi dell'articolo 28, paragrafo 3, del PAuswG, il ricorrente dovrà ottenere il rilascio di una nuova carta d'identità al più tardi alla scadenza del periodo di validità, fissato in 10 anni. Inoltre, in base all'articolo 6, paragrafo 2,

del PAuswG, il ricorrente può richiedere una nuova carta d'identità prima della scadenza della validità di una carta d'identità qualora venga dimostrato un interesse legittimo al nuovo rilascio. In caso di chip difettoso, non è più utilizzabile la funzione di identificazione online. È altresì precluso il controllo automatizzato alle frontiere. Tale limitata possibilità di utilizzazione può fondare un interesse legittimo ad un nuovo rilascio.

- 7 Il Collegio remittente dubita della conformità dell'articolo 3, paragrafo 5, del regolamento (UE) 2019/1157 al diritto dell'Unione. Tali perplessità traggono origine tanto dal fatto che detto regolamento è stato adottato secondo la procedura legislativa ordinaria, quanto dalla compatibilità dell'articolo 3, paragrafo 5, del medesimo regolamento con gli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta») e, infine, dalla carenza di una decisione valutazione ai sensi dell'articolo 35, paragrafo 10, del RGPD.
- 8 Il Collegio remittente è persuaso che, ai fini dell'adozione del regolamento (UE) 2019/1157, avrebbe dovuto trovare attuazione la procedura legislativa speciale prevista dall'articolo 77 TFUE.
- 9 L'articolo 289 TFUE opera una differenziazione tra procedura legislativa ordinaria e procedure legislative speciali. Il regolamento (UE) 2019/1157 ha il suo fondamento nell'articolo 21, paragrafo 2, TFUE ed è stato adottato secondo la procedura legislativa ordinaria. L'articolo 21, paragrafo 2, TFUE dispone che il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, possono adottare disposizioni intese a facilitare l'esercizio del diritto di circolare liberamente, quando un'azione dell'Unione risulti necessaria per raggiungere detto obiettivo e salvo che i trattati non abbiano previsto poteri di azione a tal fine.
- 10 L'articolo 77, paragrafo 3, prima frase, TFUE contiene un'ulteriore norma sulla competenza che si riferisce, in particolare, alle disposizioni relative alle carte d'identità. In base ad essa, se un'azione dell'Unione risulta necessaria per facilitare l'esercizio del diritto di circolare liberamente e salvo che i trattati non abbiano previsto poteri di azione a tale scopo, il Consiglio, deliberando secondo una procedura legislativa speciale, può adottare disposizioni relative ai passaporti, alle carte d'identità, ai titoli di soggiorno o altro documento assimilato. Il Consiglio delibera all'unanimità previa consultazione del Parlamento europeo. Il requisito dell'unanimità lascia agli Stati membri il massimo grado di sovranità in tale settore.
- 11 L'articolo 77 TFUE corrisponde al precedente articolo 62 TCE (trattato CE), sul quale il legislatore del regolamento (CE) 2252/2004, il cui articolo 1, paragrafo 2, dispone che le impronte digitali vengano memorizzate nei passaporti, fondava l'adozione di detto regolamento. Nella sentenza del 17 ottobre 2013, Schwarz (C-291/12, EU:C:2013:670), la Corte di giustizia dell'Unione europea ha affermato che l'articolo 62, punto 2, lettera a), TCE costituirebbe un fondamento

giuridico adeguato ai fini dell'adozione del regolamento (CE) 2252/2004, in particolare del suo articolo 1, paragrafo 2.

- 12 La competenza stabilita dall'articolo 77, paragrafo 3, TFUE prevale sull'articolo 21, paragrafo 2, TFUE, in quanto la prima disposizione, essendo più specifica nel contenuto, pone requisiti più elevati alla procedura legislativa e la seconda disposizione è applicabile salvo che i trattati non abbiano previsto poteri di azione allo scopo di agevolare la libera circolazione delle persone. Il regolamento (UE) 2019/1157, pur non facendo riferimento all'ulteriore sviluppo dell'acquis di Schengen, considera però, al pari del regolamento (CE) 2252/2004, l'armonizzazione delle caratteristiche di sicurezza e l'inserimento di identificatori biometrici come una tappa importante verso l'utilizzo di nuovi elementi in prospettiva di futuri sviluppi a livello europeo. Come nel caso del regolamento (CE) 2252/2004, tale normativa è intesa a rendere più sicuri i documenti (nel caso in esame: carte d'identità in luogo dei passaporti).
- 13 Alla luce di quanto precede, il Collegio remittente ritiene che un'efficace adozione del regolamento (UE) 2019/1157 – e quindi anche del suo articolo 3, paragrafo 5 – avrebbe richiesto la procedura legislativa speciale di cui all'articolo 77, paragrafo 3, TFUE.
- 14 Inoltre, permangono dubbi sulla conformità del prelievo e della conservazione delle impronte digitali nelle carte d'identità agli articoli 7 e 8 della Carta.
- 15 L'articolo 7 della Carta dispone che ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni. Dal successivo articolo 8 discende il diritto di ogni persona alla protezione dei dati di carattere personale che la riguardano.
- 16 Già nella sentenza del 17 ottobre 2013, Schwarz (C-291/12, EU:C:2013:670, punti 27 e 30), la Corte di giustizia dell'Unione europea, richiamando la sentenza della CEDU del 4 dicembre 2008, S. e Marper/Regno Unito (*Reports of judgments and decisions* 2008-V, pag. 213, punti 68 e 84), ha affermato che il prelievo e la conservazione delle impronte digitali nei passaporti da parte delle autorità nazionali, come disciplinati dall'articolo 1, paragrafo 2, del regolamento 2252/2004, costituiscono un pregiudizio ai diritti al rispetto della vita privata e alla tutela dei dati personali. Le impronte digitali costituiscono dati personali in quanto contengono obiettivamente informazioni uniche su persone fisiche e consentono la loro precisa identificazione. Gli stessi diritti fondamentali sono incisi dal prelievo e dalla conservazione delle impronte digitali nelle carte d'identità.
- 17 Il Collegio remittente dubita che il prelievo delle impronte digitali e quindi una violazione degli articoli 7 e 8 della Carta, in particolare con riguardo all'articolo 52 e all'articolo 8, paragrafo 2, della Carta, siano giustificati anche per le carte d'identità. L'articolo 8, paragrafo 2, della Carta dispone che i dati personali

devono essere trattati in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge.

- 18 Nel caso in questione, il Collegio remittente – in linea con la pronuncia della Corte di giustizia dell'Unione europea in merito ai passaporti – è persuaso del fatto che i richiedenti una carta d'identità non abbiano prestato consenso al prelievo delle loro impronte digitali. Tuttavia, l'articolo 3, paragrafo 5, del regolamento (UE) 2019/1157 lo impone come disposizione di legge con riguardo a tutte le carte d'identità.
- 19 In forza dell'articolo 1, paragrafo 1, prima frase, del PAuswG, tutti i tedeschi sono tenuti ad avere un documento d'identità valido allorché compiono i 16 anni di età e sono soggetti all'obbligo generale di registrazione oppure allorché, senza essere soggetti a tale obbligo, risiedono prevalentemente in Germania. Il rilevamento delle impronte digitali è quindi obbligatorio ai fini del rilascio di detto documento. L'esistenza di un obbligo di possesso di una carta d'identità non consente di inferire che il rispettivo richiedente abbia acconsentito a tale trattamento dei dati (in tal senso anche la sentenza della Corte del 17 ottobre 2013, Schwarz, C-291/12, EU:C:2013:670, punto 31).
- 20 L'articolo 52, paragrafo 1, della Carta, richiede pertanto un fondamento **legittimo** previsto dalla legge.
- 21 È pur vero che l'inserimento delle impronte digitali nelle carte d'identità è previsto dalla legge all'articolo 3, paragrafo 5, del regolamento (UE) 2019/1157. Ciò risulta altresì conforme, almeno in parte, agli obiettivi di interesse pubblico riconosciuti dall'Unione, come esplicitato nei considerando 1, 2, 4, 18 e 46.
- 22 All'interno dell'Unione europea, la carta d'identità può essere usata per l'attraversamento delle frontiere. Inoltre, anche alcuni Stati che non appartengono all'Unione europea, quali Svizzera, Islanda, Norvegia, Albania e Montenegro, consentono l'ingresso con la carta d'identità. In tale contesto, la carta d'identità è utilizzata quantomeno anche come documento di viaggio, cosicché la disposizione è diretta altresì a impedire l'ingresso illegale da detti paesi. Ciò costituirebbe un obiettivo d'interesse generale riconosciuto dall'Unione (sentenza della Corte del 17 ottobre 2013, Schwarz, C-291/12, EU:C:2013:670, punto 38). Tuttavia, lo scopo principale della carta d'identità non consiste, in primo luogo, nell'essere utilizzata come documento di viaggio nell'area Schengen al pari del passaporto. A tal riguardo, correttamente i considerando del regolamento (UE) 2019/1157, a differenza di quelli del regolamento 2252/2004, non fanno alcun riferimento allo spazio Schengen come spazio di libertà.
- 23 Nemmeno il regolamento (UE) 2019/1157 regola l'utilizzazione dei dati biometrici memorizzati nel senso suesposto, essendo stabilito dal suo articolo 11, paragrafo 6, che i dati biometrici conservati possono essere usati esclusivamente allo scopo di verificare l'autenticità o l'identità del titolare. Pertanto, detto regolamento non disciplina il modo in cui debba essere agevolata la libera

circolazione. Lo scopo di impedire l'ingresso illegale non può essere quindi equiparato all'agevolazione della libera circolazione.

- 24 Pur se il regolamento perseguisse una finalità di interesse generale, resterebbe però da chiarire se l'articolo 3, paragrafo 5, del regolamento (UE) 2019/1157 sia proporzionato. Tale sarebbe il caso unicamente qualora le restrizioni a tali diritti conferiti dalla Carta fossero proporzionate agli scopi perseguiti dal regolamento (UE) 2019/1157 e quindi all'obiettivo di impedire l'ingresso illegale di persone nel territorio dell'Unione e di consentire l'identificazione affidabile del titolare della carta d'identità. A tal fine, i mezzi impiegati da tale regolamento devono essere idonei a realizzare tali obiettivi e non devono eccedere quanto necessario per raggiungerli (sentenza della Corte del 17 ottobre 2013, Schwarz, C-291/12, EU:C:2013:670, punti 38 e 40).
- 25 Il Collegio remittente ritiene, dunque, che occorra tener conto del fatto che la carta d'identità non può essere equiparata al passaporto sotto il profilo fattuale e giuridico, esistendo notevoli differenze con riguardo all'uso di tali documenti. Tuttavia, l'articolo 3, paragrafo 5, del regolamento (UE) 2019/1157 considera i due documenti allo stesso modo con riguardo alle impronte digitali.
- 26 Sebbene la carta d'identità – come già esposto supra – possa essere utilizzata anche come documento di viaggio, nondimeno le carte d'identità e i passaporti differiscono sotto il profilo sia giuridico sia fattuale. Le carte d'identità sono sì usate anche come documenti di viaggio nel contesto della libera circolazione, tuttavia non è effettuato alcun controllo abituale, almeno in caso di viaggi tra gli Stati membri dell'Unione europea. Inoltre, per la maggior parte dei cittadini dell'Unione, la funzione primaria della carta d'identità nazionale non dovrebbe essere correlata alla libera circolazione. Peraltro, le carte d'identità sono suscettibili di modalità di utilizzazione non limitate a quest'ultima. Ad esempio, le carte d'identità sono usate nella vita quotidiana per interagire con le autorità amministrative nazionali o con terzi privati, come le banche o le compagnie aeree. I cittadini dell'Unione che vogliono esercitare la loro libera circolazione possono farlo già con il loro passaporto (in tal senso anche il parere del Garante europeo della protezione dei dati sulla prevista inclusione della conservazione delle impronte digitali nelle carte d'identità del 10 agosto 2018).
- 27 In Germania è altresì obbligatorio avere una carta d'identità, ai sensi dell'articolo 1, paragrafo 1, prima frase, del PAuswG. A differenza del passaporto, i cittadini non possono decidere in autonomia se richiedere o meno una carta d'identità. Il Garante europeo della protezione dei dati ritiene inoltre che l'inserimento e la conservazione delle impronte digitali avrebbe un impatto esteso su 370 milioni di cittadini dell'Unione, in quanto richiederebbe il rilevamento obbligatorio delle impronte digitali dell'85% della popolazione dell'Unione europea. Tale ampio ambito di applicazione, congiuntamente ai dati molto sensibili trattati (immagini del volto in combinazione con le impronte digitali), richiede un attento esame basato su un rigoroso criterio di necessità. Il Collegio remittente concorda con le osservazioni del Garante europeo della protezione dei dati secondo cui, date le

differenze tra passaporti e carte d'identità, l'introduzione per queste ultime di caratteristiche di sicurezza che possono essere considerate appropriate per i passaporti, non può essere effettuata automaticamente, ma richiede una riflessione e un'analisi approfondita, che manca nel caso in esame.

- 28 Secondo il Collegio remittente, in combinazione con gli ampi usi possibili descritti supra e il gran numero di cittadini dell'Unione interessati, ciò si traduce in un'intensità di pregiudizio molto più elevata rispetto ai passaporti, a fronte della quale occorre anche una giustificazione più rigorosa.
- 29 Nell'interpretare gli articoli 7 e 8 della Carta, occorre tener conto altresì dei valori del GDPR, come enunciati dai suoi considerando 1 e 2.
- 30 Ai sensi dell'articolo 9, paragrafo 1, del RGPD, i dati dattiloscopici sono particolari tipi di dati personali, segnatamente dati biometrici, i quali sono definiti dall'articolo 4, punto 14, del RGPD come dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici. In base al summenzionato articolo 9, paragrafo 1, il trattamento di tali dati biometrici è vietato, in linea di principio, ed è consentito solo in pochi casi eccezionali.
- 31 Nella misura in cui le impronte digitali devono essere inserite nelle carte d'identità al fine di promuovere la sicurezza contro la falsificazione, il parere del Garante europeo della protezione dei dati sulla prevista inclusione della conservazione delle impronte digitali nelle carte d'identità sottolinea che nel periodo dal 2013 al 2017 sono state rilevate solo 38 870 carte d'identità falsificate e che l'uso di queste ultime è in calo da anni.
- 32 Non è ancora sufficientemente chiaro se l'inserimento delle impronte digitali sia effettivamente in grado di promuovere la sicurezza contro la falsificazione. Una corrispondenza dei dati biometrici memorizzati sul chip della carta d'identità con le impronte digitali del possessore della carta d'identità conferma semplicemente che il documento appartiene al possessore. La coincidenza non costituisce di per sé una prova d'identità finché non sia verificata l'autenticità della carta d'identità stessa. È peraltro riconosciuto che l'uso di dati biometrici riduce la probabilità di successo della falsificazione di un documento, potendo pertanto l'inserimento delle impronte digitali, almeno in parte, promuovere tale obiettivo.
- 33 Tuttavia, appare alquanto dubbio che tale eventualità sia idonea a giustificare un pregiudizio di vasta portata, soprattutto perché, contrariamente al regolamento (UE) 2019/1157, una carta d'identità con un chip difettoso mantiene la sua validità secondo la normativa tedesca. A tal proposito, il Bundesamt für Sicherheit in der Informationstechnik (Ufficio federale tedesco per la sicurezza dell'informazione) dichiara che «una carta d'identità con un chip non funzionante [mantiene] la sua validità anche qualora il chip integrato sia chiaramente difettoso. La sicurezza del documento d'identità è garantita dalle caratteristiche fisiche di

sicurezza». Ove la sicurezza sia però fornita solo da queste ultime (in particolare microscritture, stampe UV, ecc.), si pone in modo ancora più evidente la questione della necessità di inserire le impronte digitali.

- 34 Lo stesso Garante europeo della protezione dei dati ha sottolineato che le misure di sicurezza relative alla stampa del documento, quale, ad esempio, l'uso di ologrammi o filigrane, avrebbero un'intensità lesiva decisamente inferiore. I metodi menzionati non implicherebbero il trattamento di dati personali, ma sarebbero altresì idonei ad impedire la falsificazione di documenti d'identità e a verificare l'autenticità di un documento.
- 35 In tale contesto, occorre inoltre tener conto di uno dei principi più importanti del diritto dell'Unione in materia di protezione dei dati: il principio della minimizzazione dei dati, in base al quale, la raccolta e l'uso dei dati personali devono essere proporzionati e necessari, nonché limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
- 36 Nel caso in cui il prelievo delle impronte digitali sia inevitabile, si pone altresì la questione del motivo per il quale sia necessaria la riproduzione dell'intera impronta. Tale prescrizione promuove l'interoperabilità tra i diversi tipi dei sistemi di riconoscimento delle impronte digitali, i quali possono essere suddivisi in tre sottocategorie. Da un lato, ci sono i sistemi che memorizzano e confrontano le immagini integrali delle impronte digitali. Altri sistemi usano le cosiddette minuzie, le quali descrivono un sottoinsieme di caratteristiche ottenute dalle immagini delle impronte digitali. Nella terza categoria rientrano i sistemi che operano con singoli modelli estratti da immagini delle impronte digitali. Laddove venisse memorizzata soltanto una minuzia, uno Stato membro che opera con un sistema che utilizza l'immagine dell'intera impronta digitale non sarebbe in grado di utilizzarla. La memorizzazione dell'intera impronta digitale promuove l'interoperabilità, aumentando però la quantità di dati personali conservati e quindi il rischio di furto di identità in caso di fuga di dati.
- 37 I chip RFID utilizzati nelle carte d'identità possono essere letti eventualmente anche da scanner non autorizzati. Ciò è dovuto al fatto che essi si attivano tramite onde radio e successivamente trasmettono i dati in forma criptata. Così, la sicurezza della procedura dipende, in definitiva, dalla qualità della tecnologia di trasmissione e di crittografia. Proprio l'uso dell'intera impronta digitale rende più elevato il rischio a tal riguardo.
- 38 Alla luce di quanto precede va altresì rilevato che le impronte digitali sono dati biometrici. Il legislatore ha dimostrato, in particolare, attraverso l'introduzione dell'articolo 9 del RGPD, che tali dati beneficiano di una protezione speciale.
- 39 Lo stesso regolamento (UE) 2019/1157 non menziona la «caratteristica di sicurezza» dell'impronta digitale nel caso di minori di età inferiore a dodici anni ed esenta del tutto i minori di età inferiore a sei anni dall'obbligo di rilevamento (articolo 3, paragrafo 7, di detto regolamento). Ancora più rilevante è però il fatto

che le persone per cui il rilevamento delle impronte digitali è fisicamente impossibile sono esentate dall'obbligo di tale rilevamento. Il regolamento in parola non si è dunque espresso sulla finalità residua di tale caratteristica di sicurezza.

- 40 Inoltre, il Garante europeo della protezione dei dati pone l'accento nel suo parere sul fatto che l'articolo 35, paragrafo 10, del RGPD si applica all'acquisizione e al trattamento delle impronte digitali. Ai sensi dell'articolo 35, paragrafo 1, di detto regolamento, è necessaria una valutazione dell'impatto sulla protezione dei dati personali, prima di procedere a un trattamento che può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Detta valutazione dovrebbe tener conto, in particolare, dei rischi per i diritti e le libertà degli interessati e delle misure di prevenzione di tali rischi, quali garanzie e misure di sicurezza.
- 41 In considerazione della base giuridica di diritto dell'Unione cui il titolare del trattamento è soggetto e del fatto che tali disposizioni disciplinano il trattamento specifico, la valutazione d'impatto generale deve essere effettuata nell'ambito dell'adozione di tale base giuridica (articolo 35, paragrafo 10, del RGPD). Una simile valutazione avrebbe dovuto essere effettuata al momento dell'adozione del regolamento (UE) 2019/1157. In base al tenore dei considerando, non risulta che essa abbia avuto luogo.
- 42 Il Collegio remittente, come il Garante europeo della protezione dei dati nel suo parere, ritiene che la valutazione d'impatto non costituirebbe il fondamento dell'inserimento obbligatorio di un'immagine del volto e di (due) impronte digitali nelle carte d'identità. Già nella procedura legislativa, il medesimo Garante suggeriva di esaminare nuovamente la necessità e la proporzionalità del trattamento dei dati biometrici (immagine del volto in combinazione con le impronte digitali) in tale contesto.
- 43 Il legislatore del regolamento prende in considerazione tale problematica concernente il RGPD nel considerando 40 solo in termini molto generici. Le espressioni sono indeterminate, come ad esempio il fatto che i cittadini dell'Unione dovrebbero essere informati sul supporto di memorizzazione e che occorrerebbe specificare ulteriormente le garanzie applicabili ai dati personali trattati e in particolare ai dati sensibili quali gli identificatori biometrici. Il supporto di memorizzazione dovrebbe garantire un elevato livello di sicurezza e una protezione efficace dall'accesso non autorizzato dei dati personali in esso contenuti. Resta vago cosa si intenda per «elevato livello di sicurezza» e quale forma debbano assumere le garanzie e le misure di sicurezza. In particolare, non risulta alcuna valutazione dei rischi derivanti da una fuga di dati del chip e dalla violazione degli articoli 7 e 8 della Carta.
- 44 Si pone pertanto la questione se l'omissione di una valutazione obbligatoria dell'impatto dei rischi consenta di lasciare impregiudicata l'efficacia di una norma oppure se, ove tale obbligo incomba sul legislatore, detta omissione implichi

invece la conseguente invalidità della disposizione. In caso contrario, il legislatore otterrebbe un premio per la sua negligenza.

DOCUMENTO DI LAVORO