ARTICOLO 29 - Gruppo per la tutela dei dati personali

01911/07/IT
WP 140

Parere 7/2007 sugli aspetti relativi alla protezione dei dati con riferimento al Sistema di informazione del mercato interno (IMI)

Adottato il 21 settembre 2007

INDICE

1. Introduzione

Il progetto di istituire un sistema informatico per lo scambio di informazioni riguardanti i dati personali suscita notevoli preoccupazioni sotto il profilo dei diritti fondamentali degli individui, ed in particolare del diritto alla privacy.

Vista la complessità del Sistema di informazione del mercato interno (*Internal Market Information system* o IMI) e dei vari aspetti associati, la DG Mercato interno della Commissione europea ha chiesto il parere del gruppo di lavoro istituito dall'articolo 29 (WP29). Il parere del gruppo si incentrerà sulle stesse tematiche trattate nei documenti *Issue paper on Data Protection in IMI* (D-4784) e *General Overview* (D-1804). Il presente parere è pertanto finalizzato ad analizzare le implicazioni del sistema IMI per quanto riguarda i dati personali tutelati a norma della direttiva 95/46/CE ("direttiva sulla tutela dei dati") e del regolamento (CE) n. 45/2001 ("regolamento sulla tutela dei dati").

> Nel marzo del 2006 i rappresentanti degli Stati membri riuniti nell'ambito del Comitato consultivo per il mercato interno hanno dato il via allo sviluppo del Sistema di informazione del mercato interno (IMI) inteso a migliorare la comunicazione tra le amministrazioni degli Stati membri. Si tratta di uno strumento informatico che offre un sistema di scambio di informazioni in grado di rendere più efficace la cooperazione quotidiana tra gli Stati membri nell'attuazione della legislazione sul mercato interno nei settori disciplinati dalla direttiva 2006/123/CE[1] relativa ai servizi nel mercato interno e dalla direttiva 2005/36/CE relativa al riconoscimento delle qualifiche professionali[2]. L'IMI è stato concepito come ausilio per superare ostacoli pratici che frenano la comunicazione e la cooperazione tra le amministrazioni dei vari Stati membri, quali le differenze tra le culture amministrative e di lavoro, le differenze linguistiche e l'assenza di interlocutori chiari nei vari Stati membri; ha inoltre lo scopo di ridurre gli oneri amministrativi e di aumentare l'efficienza e l'efficacia della cooperazione quotidiana tra gli Stati membri.

L'importanza di accentuare la cooperazione amministrativa tra gli Stati membri è un aspetto riconosciuto dalla strategia di Lisbona rinnovata[3] e dal programma dell'UE su come legiferare meglio[4] perché è un elemento che servirà a migliorare l'applicazione del diritto comunitario da parte degli Stati membri.

Questi ultimi hanno infatti il compito di garantire il funzionamento efficace e fluido della legislazione sul mercato interno nel proprio territorio, ma per fare questo devono disporre di strumenti per lavorare insieme e con la Commissione, perché solo così sarà possibile trarre tutti i benefici che il quadro legislativo riserva ai cittadini e alle imprese. L'IMI viene creato per rispondere a questa esigenza e per ottemperare all'obbligo istituito dall'articolo 34, paragrafo 1, della direttiva 2006/123/CE relativa ai servizi nel mercato interno (di seguito "direttiva sui servizi") che prevede l'istituzione di un sistema elettronico per lo scambio di informazioni tra Stati membri.

---

[1] GU L 376 del 27.12.2006, pag. 36.

[2] GU L 255 del 30.9.2005, pag. 22.

[3] Cfr. pag. 18 del documento COM (2006) 30 def., "È ora di cambiare marcia - Il nuovo partenariato per la crescita e l'occupazione".

[4] Cfr. pag. 3 del documento COM (2006) 689 def., "Esame strategico del programma per legiferare meglio nell'Unione europea".

La priorità principale nell'ambito dell'IMI sarà lo sviluppo di applicazioni ai fini della direttiva 2005/36/CE ("direttiva sulle qualifiche professionali") e della direttiva sui servizi.

2. Descrizione del sistema IMI

Il sistema, destinato principalmente alle amministrazioni e alle autorità competenti degli Stati membri, sarà costituito da una serie di applicazioni "orizzontali" che offriranno sostegno linguistico e uno strumento di comunicazione tra autorità competenti, e da applicazioni "verticali" a supporto di normative specifiche. L'IMI sarà un sistema a sé stante e tutte le sue funzioni saranno accessibili attraverso una pagina web.

2.1 Architettura: funzioni della Commissione e sistemi nazionali

Da un punto di vista strutturale, il sistema IMI si prefigge in via prioritaria di agevolare l'adempimento degli obblighi giuridici che incombono agli Stati membri per quanto riguarda lo scambio di informazioni, ma consentirà anche formule di cooperazione amministrativa nuove e più complesse. L'IMI fornirà una funzione di ricerca che permetterà di individuare l'autorità competente responsabile in un altro Stato membro e vari menu pretradotti contenenti una serie di domande strutturate per agevolare lo scambio di informazioni richiesto. Il WP29 sottolinea un aspetto cruciale: la Commissione deve concepire e preparare i menù e le domande strutturate in modo da ridurre al minimo il rischio di raccogliere informazioni non pertinenti, sproporzionate o riguardanti terzi. D'altra parte è altrettanto importante che gli utenti del sistema (ad esempio le autorità competenti che si scambiano le informazioni) garantiscano di non utilizzare il sistema per scambiarsi dati non importanti, eccessivi o dati riguardanti terzi.

Il sistema è concepito per tener conto delle varie modalità di organizzazione delle amministrazioni nazionali dei vari Stati membri (ad esempio sistemi centralizzati o decentrati, a vari livelli) e permette pertanto a questi ultimi di personalizzare l'organizzazione delle proprie autorità competenti ai fini dell'IMI, per renderlo il più efficace possibile.

Segue una presentazione dei principali soggetti che intervengono in quest'ambito; a tal fine si fa riferimento al documento *General Overview*.

2.2 Autorità coinvolte

I principali soggetti interessati dal sistema IMI saranno le autorità competenti di tutto lo Spazio economico europeo (SEE) che utilizzeranno l'IMI per scambiarsi informazioni sui settori della legislazione in materia di mercato interno riguardanti le professioni e i servizi regolamentati.

Per quanto riguarda il ruolo e i poteri di ciascuna autorità in fase di trattamento dei dati personali, è necessario sottolineare che sia la Commissione europea che i singoli Stati membri svolgeranno una funzione importante nel sistema IMI. Ciascuno Stato membro avrà infatti la possibilità di progettare le proprie strutture in modo che queste soddisfino le proprie esigenze specifiche, ma tutti gli Stati membri dovranno svolgere la stessa funzione nel contesto IMI.

Le funzioni specifiche delle autorità sono descritte nel seguente testo tratto dal documento della Commissione dal titolo *Data Protection in IMI*.

2.2.a Commissione europea

Il documento *Data Protection in IMI* stabilisce quanto segue: "*Il database si troverà su un server della Commissione a Lussemburgo. Tutti gli scambi di dati avverranno attraverso questo server e i dati scambiati saranno memorizzati sul server. I compiti della Commissione [che in genere saranno delegati all'amministratore UE del sistema] riguarderanno la registrazione del coordinatore nazionale IMI in ciascuno Stato membro, la gestione del database a livello di sistema, la gestione delle domande predefinite in base alla legislazione e la traduzione delle componenti del sistema IMI in tutte le lingue ufficiali dell'UE."*

La responsabilità per l'immissione dei dati, la conformità alle modalità di utilizzo dei dati e alle norme di qualità, la notifica e la gestione dei diritti di accesso, correzione e cancellazione ricade invece sulle amministrazioni nazionali.

Il WP29 sottolinea che, dato che la Commissione svolgerà anche determinati compiti di trattamento dei dati i) per conto degli Stati membri (ad esempio l'archiviazione e la cancellazione) e ii) per proprio conto in veste di amministratore del sistema (dati riguardanti gli utenti dell'IMI e i contatti), essa deve condividere con le autorità competenti degli Stati membri la responsabilità in materia di conformità alle normative applicabili per la protezione dei dati. Occorre inoltre definire chiaramente le mansioni e le responsabilità della Commissione e delle autorità competenti degli Stati membri.

2.2.b Autorità competente (AC)

Nello stesso documento si precisa, in merito alle autorità competenti, che "*in ciascuno Stato membro le pubbliche amministrazioni saranno nominate autorità competenti [e potranno essere responsabili di vari ambiti della normativa]. Dopo essersi registrate nel sistema, le AC potranno inviare e ricevere le richieste d'informazione attraverso l'IMI.*" A prescindere dalle relazioni che hanno con i DIMIC (negli Stati membri che decidano di designarli), tutte le AC di uno Stato membro saranno soggette alla vigilanza del NIMIC dello Stato membro in questione[5].

Il WP29 sottolinea che in alcuni Stati membri non sempre le informazioni di cui ha bisogno l'AC richiedente riguardo ad un determinato lavoratore o prestatore di servizi migrante sono detenute da un'unica AC. Così può essere necessario fare una distinzione tra il riconoscimento dei diplomi, in cui l'autorità competente può essere un particolare ministro, e il riconoscimento delle valutazioni per il rilascio delle licenze professionali, nel qual caso l'AC potrebbe invece essere un'associazione di categoria. In casi come questi l'AC richiedente può dover contattare due autorità competenti diverse. Per affrontare questi e altri aspetti analoghi, il WP29 accoglie positivamente il fatto che chi ha progettato l'IMI abbia previsto una rete di coordinatori all'interno di ciascuno Stato membro, per aiutare le AC richiedenti a trovare gli omologhi negli altri Stati membri (cfr. punto 2.2, lettere c) e d) del presente documento). Allo stesso tempo il WP29 dichiara che l'interfaccia dell'IMI deve essere concepita in modo da ridurre al minimo il rischio di confusione sull'autorità competente responsabile di un determinato aspetto.

[5] Le funzioni del DIMIC (coordinatore delegato IMI) e del NIMIC (coordinatore nazionale IMI) saranno illustrate nel punto 2.2, lettere c) e d).

2.2.c Coordinatore nazionale IMI (NIMIC)

Ogni Stato membro nominerà un coordinatore nazionale per il sistema IMI che sarà la propria autorità IMI di massimo livello nonché l'interlocutore diretto nelle comunicazioni con la Commissione europea e con gli altri Stati membri per tutti gli aspetti tecnici connessi all'IMI e quando saranno necessari passaggi procedurali per ottenere risposte.

Come indicato nel documento *Data Protection in IMI*, il coordinatore nazionale IMI sarà in grado di visualizzare l'elenco di tutte le richieste inviate dalle AC o pervenute loro oppure quello dei coordinatori delegati IMI del proprio Stato membro; tale elenco non conterrà tuttavia dati personali.

Il WP29 accoglie favorevolmente questa limitazione visto che, come conferma la stessa Commissione, i NIMIC non hanno necessariamente l'esigenza di accedere ai dati personali per poter svolgere i compiti affidatigli. In tale contesto l'accesso ai dati personali rappresenterebbe una violazione dell'articolo 6, paragrafo 1, lettera c), della direttiva sulla tutela dei dati, secondo il quale gli Stati membri devono garantire che i dati personali trattati siano: "*adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati*."

Ciò detto, il WP29 ritiene anche necessario esplicitare tale limitazione, precisando più dettagliatamente le informazioni che devono figurare in tali elenchi.

Il WP29 è anche convinto che la ripartizione delle competenze e dei compiti tra la Commissione, i coordinatori e le autorità competenti debba essere definita con maggiore precisione, posto che loro rispettive funzioni con riferimento all'IMI si possono descrivere più opportunamente come un "controllo congiunto". Il WP29 osserva che, in certa misura, ciascun soggetto coinvolto nel sistema IMI svolgerà il duplice ruolo di incaricato del trattamento e responsabile del trattamento in alcuna forma, in funzione dell'attività di trattamento svolta in ogni determinata situazione. Il sistema IMI è complesso e può non essere sempre facile capire se i soggetti coinvolti svolgono il ruolo di responsabili o di incaricati del trattamento dei dati o entrambi. Questa possibile confusione sottolinea l'importanza di individuare in maniera esplicita e specifica l'obiettivo di ciascuna azione di trattamento dei dati: in tal modo tutte le parti potranno comprendere quali sono gli usi consentiti dei dati e sapere come conformarsi alle norme in materia di tutela dei dati anche in situazioni in cui non è chiaro quale sia la natura precisa del loro intervento o quando tale intervento sia una combinazione delle due funzioni.

2.2.d Coordinatore delegato IMI (DIMIC)

Nell'ambito del sistema è previsto un terzo tipo di funzione, a discrezione degli Stati membri, ovvero la possibilità di designare un coordinatore delegato IMI (DIMIC) incaricato di coordinare e vigilare sul ruolo svolto dalle singole autorità competenti in un unico ambito legislativo o settoriale.

Come illustrato nel documento *Data Protection in IMI*, il coordinatore delegato IMI dovrebbe poter visualizzare la lista di tutte le richieste inviate o pervenute alle AC alle quali è collegato. Come rileva il documento, la lista in questione conterrà sufficienti informazioni di livello elevato da permettere al coordinatore di monitorare il flusso delle richieste, senza tuttavia alcun legame ai dati personali. Il ruolo del DIMIC è stato concepito espressamente per

consentire agli Stati membri che hanno sistemi centralizzati di coordinarsi con gli Stati membri che hanno una struttura più decentrata o che vantano molte autorità competenti.

Il WP29 rileva che occorre chiarire e definire con maggiore precisione i diversi ruoli del NIMIC e del DIMIC nonché le loro responsabilità nel garantire un'adeguata tutela dei dati personali che vengono scambiati sotto il loro controllo, al fine di poter analizzare in maniera più conclusiva le implicazioni del loro intervento.

2.2.e Autorità collegate

Un'autorità competente può anche concedere un "*accesso a fini di monitoraggio"* ad altre amministrazioni pubbliche del proprio Stato membro. Per "*accesso a fini di monitoraggio"* s'intende che un'altra autorità può visualizzare la lista di tutte le richieste inviate dalle AC o ad esse pervenute senza accedere ad alcun dato personale trattato.

Questa funzione dovrebbe permettere alle organizzazioni di stampo professionale (come le associazioni di categoria) di visualizzare una lista anonima delle richieste destinate alle relative organizzazioni, ad esempio nell'ottica di garantire che tali richieste siano inoltrate alle AC effettivamente responsabili. Il WP29 ritiene tuttavia necessario che vengano definiti in maniera più esplicita gli obiettivi e i benefici specifici del ruolo delle autorità collegate, nonché le informazioni particolari cui esse possono accedere, per evitare che vi sia un accesso non autorizzato ai dati personali.

2.3 Ruoli e diritti all'interno del sistema

Le principali attività di trattamento dei dati avverranno all'interno del sistema IMI durante lo scambio di informazioni tra le autorità competenti degli Stati membri; accanto a tali attività vi sarà anche il trattamento dei dati personali operato dalla Commissione stessa e riguardante informazioni sulle autorità competenti. Tutti i soggetti coinvolti nel trattamento dei dati personali (AC, NIMIC o DIMIC) dovranno sempre operare nel rispetto delle normative nazionali che attuano la direttiva 95/46/CE[6] nello Stato membro in cui hanno sede. A sua volta, la Commissione è tenuta al rispetto del regolamento sulla tutela dei dati.

Vista la diversità dei ruoli e dei soggetti coinvolti nel sistema IMI è necessario stabilire quali sono i tipi di trattamento dati di cui ciascun soggetto è considerato il "responsabile del trattamento". La definizione di "responsabile del trattamento" figura all'articolo 2, lettera d), della direttiva sulla tutela dei dati e recita: "*la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali*."

D'altro canto la medesima direttiva, all'articolo 2, lettera e), definisce così l'"incaricato del trattamento": "*la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento*." L'incaricato è pertanto la persona o l'autorità che tratta effettivamente i dati seguendo le istruzioni del responsabile del trattamento.

Sempre la direttiva sulla tutela dei dati stabilisce, all'articolo 17, paragrafo 3, che l'esecuzione dei trattamenti da parte di terzi (cioè da parte di un soggetto diverso dal responsabile del trattamento) deve essere disciplinata da un contratto o da un atto giuridico che vincoli

[6] GU L 281 del 23.11.1995, pag. 31.

l'incaricato del trattamento al responsabile del trattamento e che preveda segnatamente che l'incaricato del trattamento operi soltanto su istruzioni del responsabile del trattamento.

Nel presente documento non verranno esaminati approfonditamente tutti i possibili scenari di trattamento dei dati; tuttavia, il WP29 ritiene che, per ogni intervento di trattamento, il responsabile del trattamento ha il compito di assicurare il rispetto dei principi e delle garanzie istituite nel presente documento, anche per quanto riguarda le misure di sicurezza. L'incaricato del trattamento, da parte sua, deve rispettare gli obblighi di riservatezza adottando tutte le misure di sicurezza del caso e agendo solo su istruzione del responsabile del trattamento.

Le autorità competenti e la Commissione devono essere chiaramente consapevoli che la memorizzazione e la cancellazione dei dati sono operazioni di cui condividono la responsabilità. In tal senso occorrerà pertanto preparare un documento che definisca la cornice in cui si inseriscono i rapporti tra responsabile e incaricato del trattamento per quanto riguarda le due operazioni indicate, con una chiara descrizione dei compiti e delle responsabilità di ciascuna parte.

La struttura dell'IMI crea una rete notevolmente complessa di responsabili e incaricati del trattamento dei dati. È dunque necessario capire che le responsabilità delle singole parti possono variare in funzione del tipo di attività interessata e non sempre è necessariamente chiaro se un soggetto è il responsabile o l'incaricato del trattamento. È evidente che, a prescindere da questa distinzione, tutti i soggetti che sono responsabili o effettuano direttamente il trattamento devono mantenere il livello di sicurezza dei dati e rispettare i principi di trattamento dei dati indicati nella direttiva o nel regolamento sulla tutela dei dati, secondo il caso.

3. Dati personali trattati

Il sistema IMI può avere ripercussioni sui diritti fondamentali di un numero consistente di lavoratori e prestatori di servizi migranti che esercitano il proprio diritto alla libera circolazione nell'UE. Il sistema conserva anche dati sugli utenti dell'IMI (personale delle AC, NIMIC e DIMIC).

L'articolo 2 della direttiva sulla tutela dei dati definisce i dati personali come "*qualsiasi informazione concernente una persona fisica identificata o identificabile.*"[7] Poiché il sistema IMI tratta e archivia i dati personali per due finalità diverse, il WP29 ritiene di poter concludere che il sistema prevede due categorie diverse di trattamento dei dati personali.

- La prima categoria riguarda i dati personali delle AC (e dei NIMIC e DIMIC) che utilizzeranno l'IMI. Poiché si tratta delle coordinate degli utenti, il sistema memorizzerà nomi, numeri di telefono, indirizzi di posta elettronica e altre informazioni analoghe. L'elenco dei dati che saranno raccolti da queste persone deve essere indicato specificamente e deve rispondere alla disposizione contemplata dalla direttiva, secondo la quale i dati non devono essere eccedenti rispetto a quelli necessari per la funzionalità del sistema (qualità dei dati).

- La seconda categoria di trattamento riguarda invece i lavoratori e i prestatori di servizi nel contesto della direttiva sui servizi e della direttiva sulle qualifiche professionali. Tali dati comprendono nome, numero di telefono, indirizzo di posta elettronica, data di nascita e

[7] Sul concetto di dati personali cfr. il parere 4/2007, WP 136.

nazionalità di ciascun prestatore di servizi (se del caso, e in genere a fini di identificazione) nonché dati relativi alle qualifiche professionali e dati più sensibili come quelli sulla buona condotta, sulle azioni disciplinari, sulle sanzioni penali e sulla legalità dello stabilimento.

4. Analisi del sistema sotto il profilo giuridico e aspetti specifici

4.1 Base giuridica per il trattamento dei dati personali (Articolo 7)

Le direttive sulle qualifiche professionali e sui servizi creano obblighi specifici in materia di cooperazione amministrativa tra Stati membri, come l'obbligo di scambiarsi informazioni, che nella maggior parte dei casi riguardano "*una persona fisica identificata o identificabile*." Ciò significa che il relativo quadro legislativo subirà modifiche sostanziali man mano che queste direttive saranno recepite nell'ordinamento nazionale. Tuttavia le norme da introdurre per quanto riguarda l'IMI devono essere coerenti con i principi generali di tutela dei dati definiti nella direttiva e nel regolamento in materia già citati.

Il sistema IMI determinerà, inevitabilmente, effetti più rilevanti sui meccanismi di trattamento dei dati e sulle relative attività di vigilanza e controllo affidate alle autorità competenti.

L'articolo 56 della direttiva sulle qualifiche professionali recita:

"*1. Le autorità competenti dello Stato membro ospitante e di quello d'origine collaborano strettamente e si assistono reciprocamente per agevolare l'applicazione della presente direttiva. Essi garantiscono la riservatezza delle informazioni che scambiano.*

"*2. Le autorità competenti dello Stato membro ospitante e dello Stato membro d'origine si scambiano informazioni concernenti l'azione disciplinare o le sanzioni penali adottate o qualsiasi altra circostanza specifica grave che potrebbero avere conseguenze sull'esercizio delle attività previste dalla presente direttiva, nel rispetto della normativa sulla protezione dei dati personali di cui alle direttive 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, e 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).*"

Anche l'articolo 28 della direttiva sui servizi istituisce l'assistenza reciproca:

"1. Gli Stati membri si prestano assistenza reciproca e si adoperano per instaurare forme di collaborazione efficaci onde garantire il controllo dei prestatori e dei loro servizi…

"6. Gli Stati membri forniscono al più presto e per via elettronica le informazioni richieste da altri Stati membri o dalla Commissione."

La cooperazione richiesta da queste direttive deve essere attuata con diligenza, ma richiede maggiori capacità e reattività. A tal fine la direttiva sui servizi invoca la creazione di uno strumento elettronico per semplificare e accelerare lo scambio di informazioni. In particolare, l'articolo 34 della direttiva in questione stabilisce che *"[l]a Commissione, in collaborazione con gli Stati membri, istituisce un sistema elettronico per lo scambio di informazioni tra gli Stati membri tenendo conto dei sistemi di informazione esistenti.*"

Il WP29 ritiene necessario stabilire chiaramente che il sistema IMI deve rispettare le norme esistenti in materia di protezione dei dati. Questo obbligo è sancito esplicitamente nell'articolo 43 della direttiva sui servizi, che accentua l'importanza di un'applicazione continua e coerente della direttiva sulla tutela dei dati e della direttiva 2002/58/CE ("direttiva relativa alla vita privata e alle comunicazioni elettroniche").

A livello generale, la base giuridica per il trattamento dei dati negli Stati membri è contenuta nell'articolo 7 della direttiva sulla tutela dei dati, che definisce le condizioni che legittimano le attività di trattamento dei dati. L'articolo 7, lettera c), in particolare, specifica che il trattamento dei dati personali può avvenire se "*è necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento*." L'articolo 5, lettera b), del regolamento sulla tutela dei dati contiene disposizioni analoghe.

Come anticipato, l'articolo 34 della direttiva sui servizi istituisce quest'obbligo giuridico per i responsabili del trattamento dati e (una volta recepito negli ordinamenti nazionali) consente loro di trattare i dati personali del caso. Questa base giuridica solleva tuttavia alcuni potenziali aspetti problematici.

In primo luogo, la direttiva sulle qualifiche professionali non fa riferimento ad alcuno strumento elettronico per lo scambio delle informazioni, anche se prevede la cooperazione. In effetti, l'articolo 56, paragrafo 2, impone alle autorità competenti degli Stati membri di scambiarsi informazioni concernenti l'azione disciplinare o le sanzioni penali adottate o qualsiasi altra circostanza specifica grave che potrebbero avere conseguenze sull'esercizio delle attività previste dalla direttiva citata, ma non contempla la creazione di un sistema elettronico a tal fine. Altre disposizioni della direttiva prevedono anche scambi di informazioni se un'autorità competente ha fondati dubbi su un aspetto specifico. Anche se la DG MARKT ritiene che la base giuridica per lo scambio delle informazioni risieda in queste disposizioni specifiche, non è certo che esse rappresentino una base giuridica del tutto adeguata per il trattamento dei dati nel contesto del sistema IMI ai fini della cooperazione prevista dalla direttiva sulle qualifiche professionali.

In secondo luogo, affinché l'articolo 7, lettera c), della direttiva sulla tutela dei dati possa rappresentare la base giuridica per il trattamento dei dati, è necessario che le direttive sulle qualifiche professionali e sui servizi siano recepite nell'ordinamento nazionale. Se uno Stato membro non le ha recepite è ancora una volta discutibile l'esistenza di una base giuridica adeguata e, dunque, la possibilità di procedere al trattamento dei dati attraverso l'IMI.

Il WP29 aggiunge inoltre che, anche se la direttiva sui servizi e quella sulle qualifiche professionali, una volta recepite nel diritto nazionale, fornissero una base giuridica generale, occorrerebbe comunque motivare ogni singolo scambio di dati. In particolare, secondo la direttiva sulla tutela dei dati, ogni operazione di trattamento dei dati deve perseguire finalità specificate, esplicite e legittime ed essere fondata su una base giuridica adeguata specifica alla finalità perseguita.

Infine, il WP29 mette in luce che anche l'articolo 7, lettera e), della direttiva sulla tutela dei dati può essere una base giuridica complementare discutibile ai fini del trattamento dei dati; ai sensi di tale articolo, il trattamento può essere effettuato soltanto quando: *"è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati"*. Il sistema IMI è finalizzato a fornire informazioni e agevolare la cooperazione tra le varie

autorità competenti degli Stati membri. In altri termini, ha finalità d'interesse pubblico perché contribuisce a garantire il corretto funzionamento del mercato interno da parte delle persone che intendono avvalersi della libertà di stabilimento e della libertà di prestare servizi nell'ambito della propria attività professionale.

Nonostante le possibilità offerte dall'articolo 7, lettere c) ed e), alla luce delle incertezze giuridiche illustrate il WP29 raccomanda una soluzione specifica per la base giuridica, ovvero l'adozione da parte della Commissione di una decisione di attuazione, come del resto quest'ultima ha recentemente deciso di fare. Oltre a rafforzare la base giuridica per il trattamento dei dati, tale decisione dovrebbe anche definire i campi di dati da inserire nel database, il contenuto minimo delle richieste, delle risposte e dei flussi di dati e precisare i ruoli e le responsabilità dei vari soggetti coinvolti e gli obblighi giuridici sotto il profilo della tutela dei dati.

4.2 Applicazione dei principi di qualità dei dati (Articolo 6)

4.2.a Qualità e necessità dei dati

Il sistema IMI è uno strumento concepito appositamente per condividere le informazioni e consentirvi l'accesso alle autorità competenti quando fosse necessario. Comporta pertanto un flusso di informazioni, alcune delle quali sensibili (con la possibilità di conservare i dati per un periodo di sei mesi, come illustrato al punto 4.2, lettera c), del presente documento), e deve dunque rispettare i principi istituiti all'articolo 8 della direttiva sulla tutela dei dati. È stato esplicitamente stabilito che l'IMI deve rispettare le garanzie introdotte dalla direttiva sulla tutela dei dati al fine di salvaguardare i diritti legittimi delle persone interessate che sono stati recepiti nell'ordinamento nazionale di tutti gli Stati membri.

In primo luogo occorre soddisfare l'obbligo di qualità dei dati definito all'articolo 6 della direttiva sulla tutela dei dati. In base a tale principio, possono essere rilevati dati personali solo per finalità determinate, esplicite e legittime ed essere successivamente trattati in modo non incompatibile con tali finalità. Per soddisfare tale principio è dunque necessario che venga definita con chiarezza la finalità per la quale vengono rilevati e trattati i dati con il sistema IMI.

In secondo luogo occorre verificare la conformità ai principi della proporzionalità e della legittimità, tenuto conto dei rischi per la tutela dei dati, dei diritti fondamentali degli individui e soprattutto dell'eventuale necessità di divulgare informazioni relative a procedimenti disciplinari.

4.2.b Proporzionalità

La proporzionalità è un principio essenziale nel quadro giuridico istituito dalla direttiva 95/46/CE e dal regolamento (CE) n. 45/2001 e prevede che nei questionari utilizzati per lo scambio delle informazioni in ambito IMI le AC non possano fornire informazioni irrilevanti o eccessive rispetto all'obiettivo definito dello scambio. Pertanto, nell'ambito dello scambio di informazioni su un lavoratore o un prestatore di servizi migrante, la finalità deve essere definita in anticipo.

Le persone designate possono stampare una relazione completa di qualsiasi scambio di informazioni in qualsiasi lingua ufficiale dell'UE. L'IMI permetterà inoltre di caricare e archiviare eventuali documenti o immagini supplementari se rilevanti.

Inoltre, in applicazione del principio di proporzionalità, il WP29 raccomanda che l'AC responsabile del sistema IMI valuti con attenzione se possa essere opportuno limitare il numero delle persone autorizzate a inviare e a rispondere alle richieste di informazioni.

Nel contesto dell'IMI è inoltre importante che l'elenco delle domande attraverso le quali le AC potranno scambiarsi le informazioni sia elaborato tenendo conto del principio di proporzionalità. A tal fine, la soluzione più sicura sotto il profilo della tutela dei dati sarebbe quella di elencare tutti i campi di dati (cioè tutte le domande e le risposte predefinite) nella decisione di attuazione citata in precedenza (cfr. punto 4.1). Il WP29 riconosce, tuttavia, che chi progetta il sistema possa voler mantenere una certa flessibilità per consentire futuri adattamenti o miglioramenti del sistema stesso. Per trovare una soluzione a questi interessi divergenti e garantire allo stesso tempo degli scambi di informazioni trasparenti, il WP29 suggerisce che la nuova decisione di attuazione della Commissione indichi esplicitamente che: i) tutte le domande predefinite devono essere attinenti agli obblighi previsti dalle direttive sulle qualifiche professionali e sui servizi (o eventualmente da altre direttive che dovessero essere aggiunte in futuro in un allegato aggiornato alla decisione della Commissione); ii) tali domande devono essere elaborate in consultazione con i soggetti interessati degli Stati membri e iii) le domande e le risposte predefinite devono essere pubblicate sul sito web dell'IMI.

4.2.c Aspetti particolari riguardanti la conservazione dei dati personali

La Commissione intende fissare un periodo automatico di 6 mesi per la conservazione dei dati e inserire nell'architettura del sistema dei richiami automatici sulla cancellazione dei dati.

Secondo la direttiva sulla tutela dei dati personali, questi devono essere conservati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati (articolo 6, paragrafo 1, lettera e), e regolamento (CE) n. 45/2001). Questa precisazione è necessaria per garantire il rispetto del principio di proporzionalità del trattamento.

Il WP29 ritiene che i sei mesi proposti dalla Commissione possano a prima vista rappresentare un periodo ragionevole, perché può accadere che le autorità competenti debbano fare domande supplementari sullo stesso caso. Secondo il WP29 è tuttavia necessario che, nella sua decisione di attuazione, la Commissione spieghi chiaramente i motivi che giustificano la conservazione dei dati per questo periodo specifico.

4.2.c.i Conservazione dei dati da parte della Commissione

I dati archiviati sul server della Commissione a Lussemburgo devono essere soggetti a norme di tutela analoghe a quelle applicabili ai dati memorizzati nei database nazionali. In particolare, i dati in questione possono essere conservati nel sistema IMI solo finché sono necessari alle finalità per le quali sono stati rilevati.

I dati contenuti nel server non devono essere utilizzati per motivi diversi o altre richieste di informazione e devono sempre essere trattati secondo la normativa sulla protezione dei dati. In particolare è estremamente importante impedire l'accesso non autorizzato ad essi.

Se il periodo di conservazione dei dati ritenuto più opportuno (che corrisponderà dunque anche al periodo indicato all'articolo 4, lettera e), del regolamento (CE) n. 45/2001) viene fissato a 6 mesi, sarà necessario determinare in maniera chiara ed esplicita l'obiettivo o la finalità di ciascuna operazione di trattamento dei dati, oltre che garantire che non vi sia alcun accesso indebito ad essi.

4.2.c.ii Periodo di conservazione dei dati trattati e archiviati dalle autorità nazionali

Se anche le autorità nazionali conservano dati personali, questi devono essere archiviati solo fino al termine dello scambio o dell'operazione per il quale o la quale sono stati rilevati, fissando scadenze determinate per la loro cancellazione secondo quanto previsto dalla normativa nazionale di ciascuno Stato membro.

Questa disposizione è particolarmente importante in situazioni in cui un addetto dell'AC è in grado di archiviare queste informazioni sul disco fisso del proprio computer o su un altro dispositivo analogo. Anche in quel caso si applica il limite temporale fissato per la conservazione dei dati, che devono essere "bloccati" non appena non siano più utili per le finalità per le quali erano stati rilevati. Questo obbligo va naturalmente ad aggiungersi agli altri previsti dalle norme di tutela dei dati istituite a livello nazionale.

4.2.d Categorie particolari di dati

Il trattamento di dati sensibili impone di dedicare un'attenzione particolare al rispetto delle norme di protezione dei dati. Le condizioni e limitazioni riguardanti i dati sensibili sono istituite all'articolo 8 della direttiva sulla tutela dei dati e all'articolo 10 del regolamento (CE) n. 45/2001.

Questi dati comprendono indicazioni che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, come pure trattare dati relativi alla salute e alla sessualità. Anche i dati riguardanti i reati, le condanne penali o le misure di sicurezza sono ritenuti sensibili ai sensi della direttiva sulla tutela dei dati (e del regolamento (CE) n. 45/2001). Gli Stati membri possono ritenere sensibili anche i dati riguardanti le sanzioni o i procedimenti amministrativi.

Il documento *Data Protection in IMI* indica che l'IMI "*non è finalizzato*" a trattare dati sensibili di questo tipo. Tuttavia, gli scambi di informazioni che avvengono tramite il sistema possono eventualmente comprendere dati riguardanti la salute (ad esempio se la persona in cerca di lavoro è portatrice di disabilità).

Il WP29 ritiene che l'espressione "non è finalizzato" sia troppo vaga e permissiva. Per garantire la conformità alle disposizioni in materia di tutela dei dati occorre una formulazione vincolante, ad esempio: i dati sensibili "non devono essere trattati" e le eventuali deroghe devono essere indicate chiaramente ed essere soggette a ulteriori garanzie.

L'articolo 8 della direttiva sulla tutela dei dati sancisce chiaramente che "*[g]li Stati membri vietano il trattamento di dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale*". L'articolo 10 del regolamento (CE) n. 45/2001 ha una formulazione analoga.

In particolare, il paragrafo 5 dell'articolo 8 stabilisce che *"[i] trattamenti riguardanti i dati relativi alle infrazioni, alle condanne penali o alle misure di sicurezza possono essere effettuati solo sotto controllo dell'autorità pubblica, o se vengono fornite opportune garanzie specifiche, sulla base del diritto nazionale, fatte salve le deroghe che possono essere fissate dallo Stato membro in base ad una disposizione nazionale che preveda garanzie appropriate e specifiche. Tuttavia un registro completo delle condanne penali può essere tenuto solo sotto il controllo dell'autorità pubblica*.

Gli Stati membri possono prevedere che i trattamenti di dati riguardanti sanzioni amministrative o procedimenti civili siano ugualmente effettuati sotto controllo dell'autorità pubblica."

La direttiva sulle qualifiche professionali fornisce, all'articolo 56, paragrafo 2, una base giuridica per la trasmissione dei dati penali e sulle azioni disciplinari, in quanto ribadisce che tali scambi devono rispettare le disposizioni illustrate in precedenza. Tuttavia, le condizioni specifiche applicabili allo scambio di informazioni sui dati penali dovrebbero basarsi sulla normativa nazionale che attua la direttiva 95/46/CE.

"*Le autorità competenti dello Stato membro ospitante e dello Stato membro d'origine si scambiano informazioni concernenti l'azione disciplinare o le sanzioni penali adottate o qualsiasi altra circostanza specifica grave che potrebbero avere conseguenze sull'esercizio delle attività previste dalla presente direttiva, nel rispetto della normativa sulla protezione dei dati personali di cui alle direttive 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, e 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).*"

L'articolo 33 della direttiva sui servizi prevede inoltre norme specifiche per lo scambio di informazioni riguardanti l'onorabilità del fornitore di servizi migrante. Tali norme devono essere esaminate integralmente ben prima della loro attuazione per valutarne le implicazioni ai fini della protezione dei dati. "*Gli Stati membri comunicano, su richiesta di un'autorità competente di un altro Stato membro, conformemente al loro diritto nazionale, le informazioni relative alle azioni disciplinari o amministrative promosse o alle sanzioni penali irrogate e alle decisioni relative all'insolvenza o alla bancarotta fraudolenta assunte dalle loro autorità competenti nei confronti di un prestatore che siano direttamente pertinenti alla competenza del prestatore o alla sua affidabilità professionale. Lo Stato membro che comunica tali informazioni ne informa il prestatore interessato.*"

Per quanto riguarda le disposizioni giuridiche che legittimano il trattamento dei dati, è necessario tenere presenti i principi istituiti nella direttiva sulla tutela dei dati, che illustra in modo più concreto i concetti di proporzionalità, qualità e limitazioni all'uso dei dati ai fini della loro tutela. Nello scambio di dati sensibili è fondamentale garantire che le informazioni personali siano accurate e aggiornate: per esempio, non dovrebbero essere scambiati dati penali obsoleti.

Ci saranno inoltre situazioni in cui i dati relativi alle sanzioni amministrative non sono essenziali per l'esercizio di una professione in un dato Stato membro. In tal caso occorre tener conto degli statuti professionali dello Stato membro di origine e dello Stato membro in cui il

prestatore di servizi migra. A prescindere dall'importanza particolare dei dati in una situazione come questa, il trattamento dei dati in ambito IMI dovrà rispettare il principio di proporzionalità di cui alla direttiva sulla tutela dei dati[8].

Per quanto riguarda i dati sui debiti insoluti o gli illeciti penali, il documento intitolato *Working Document on Black Lists* (WP65)[9] prevede quanto segue:

"L'articolo 8, paragrafi 5 e 6, della direttiva 95/46/CE cita il trattamento di dati relativi alle infrazioni e alle condanne penali e stabilisce che, in generale, tale trattamento può essere effettuato solo sotto il controllo dell'autorità pubblica, fatte salve le deroghe che possono essere fissate dallo Stato membro in base ad una disposizione nazionale che preveda garanzie appropriate per evitare ripercussioni sui diritti fondamentali dei cittadini; tali deroghe devono essere notificate alla Commissione.

La legittimità del trattamento di fascicoli comprendenti dati sugli illeciti penali si fonda sull'obbligo delle autorità di mantenere la sicurezza e l'ordine pubblico. È indubbio che questo principio giustifica il trattamento di tali dati, a condizione tuttavia che siano rispettate le restrizioni indicate nel paragrafo precedente, come previsto dall'articolo 7, lettera e), della direttiva.

Per quanto riguarda il trattamento dei dati personali riguardanti gli illeciti penali, la maggior parte degli Stati membri dispone di archivi contenenti informazioni di questo tipo che sono tenuti sotto controllo da un'autorità pubblica…

Questo tipo di trattamento deve sempre tener conto dei principi di qualità dei dati contenuti nella direttiva, in particolare per quanto riguarda l'accuratezza e l'aggiornamento dei medesimi. Analogamente occorre prestare particolare attenzione al diritto alla correzione e alla cancellazione periodica o automatica dei dati riguardanti un soggetto una volta trascorso il periodo di tempo stabilito per legge e alla creazione, a tal fine, di vari meccanismi che rendano possibili, agevolino e accelerino queste operazioni: il mantenimento delle informazioni riguardanti una persona in tali archivi oltre i periodi fissati può infatti avere conseguenze pregiudizievoli.

Queste osservazioni sono particolarmente rilevanti nel caso di sentenze di non colpevolezza, limitazione della responsabilità o riabilitazione, per i quali non ci sarebbe alcun motivo di conservare i dati. Occorre sottolineare che gran parte degli Stati membri disciplina questi aspetti nell'ambito del proprio diritto penale e dunque i criteri applicabili a tal fine variano.

Un altro punto fondamentale da considerare è l'accesso alle informazioni, cioè il fatto di determinare quali siano le persone o le istituzioni autorizzate ad accedere ai dati contenuti in tali archivi. Le persone interessate devono avere sempre il diritto di accedere alle informazioni che li riguardano.

---

[8] Per esempio, la direttiva 2002/92/CE sulla intermediazione assicurativa stabilisce chiaramente in che misura le informazioni sulle sanzioni penali e sull'onorabilità siano importanti ai fini dell'esercizio di tale attività professionale. L'articolo 4, paragrafo 2, stabilisce così che *"[g]li intermediari assicurativi e riassicurativi devono possedere il requisito dell'onorabilità. Essi devono possedere almeno un certificato penale immacolato o analogo requisito nazionale in riferimento a gravi illeciti penali connessi con reati contro il patrimonio o altri reati in relazione ad attività finanziarie e non devono essere stati dichiarati falliti, salvo che sia intervenuta la riabilitazione a norma del diritto nazionale*."

[9] WP 65, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp65_en.pdf

Questa disposizione in materia di accesso può dar vita a situazioni alquanto complesse e problematiche: si pensi, ad esempio, al caso di una persona in cerca di occupazione alla quale, negli Stati membri in cui ciò sia consentito nell'ambito di una procedura di selezione, il datore di lavoro chieda di presentare un estratto del casellario giudiziale rilasciato dal responsabile del trattamento dei dati di un'autorità pubblica. Il candidato ottiene tale estratto, che potrebbe contenere dati su eventuali condanne penali o altri provvedimenti di sicurezza a suo carico. Il datore di lavoro avrebbe dunque accesso al contenuto di alcuni dati, diritto che non gli è direttamente riconosciuto sotto il profilo giuridico.

"*Le situazioni ipotetiche illustrate finora possono complicarsi ulteriormente se il datore di lavoro dovesse successivamente fare uso di tali informazioni, visto che, in teoria, la semplice consultazione delle informazioni fornite dal candidato durante la procedura di selezione non costituirebbe una violazione dell'articolo 8, paragrafo 5, della direttiva, mentre potrebbe esserlo un eventuale trattamento manuale o elettronico successivo*."

Per limitare al massimo la trasmissione superflua di dati di questo genere, sensibili ma non sempre rilevanti, il WP29 suggerisce che, qualora non sia strettamente necessario trasferire informazioni sul casellario giudiziale di una persona, le domande e le risposte pre-definite contenute nell'interfaccia IMI non dovrebbero prevedere la richiesta di dati penali e dovrebbero essere riformulate in modo da ridurre al minimo la condivisione di dati sensibili. Per citare un esempio, all'autorità competente del paese ospitante può bastare sapere che un avvocato migrante è registrato legalmente e regolarmente iscritto all'albo degli avvocati del paese d'origine, senza dover necessariamente essere informata dei reati al codice della strada eventualmente presenti nel casellario giudiziale di tale persona, se ciò non impedisce al lavoratore di esercitare la professione di avvocato nel paese d'origine.

4.3 Utilizzo di un numero identificativo nazionale

Il documento *Data protection in IMI* stabilisce: "*Infine, a norma dell'articolo 8, paragrafo 7, della direttiva 95/46/CE gli Stati membri determinano a quali condizioni un numero nazionale di identificazione o qualsiasi altro mezzo identificativo di portata generale può essere oggetto di trattamento. Il trattamento di dati personali di questo tipo agevola certamente lo scambio di informazioni tra le autorità competenti nel senso che è più facile identificare il prestatore di servizi interessato. Le restrizioni nazionali allo scambio di questi dati non sembrano pertanto giustificate*."

Si tratta di un tema estremamente delicato. Il trattamento dei numeri di identificazione nazionali è una prerogativa degli Stati membri, come stabilito espressamente dall'articolo 8, paragrafo 7, della direttiva sulla tutela dei dati: "*Gli Stati membri determinano a quali condizioni un numero nazionale di identificazione o qualsiasi altro mezzo identificativo di portata generale può essere oggetto di trattamento*." Gli Stati membri possono pertanto determinare tutte le condizioni e le modalità per trasmettere il numero di identificazione nazionale attraverso il sistema IMI, fissando eventualmente anche le restrizioni. In alcuni Stati membri, ad esempio, l'uso del numero di identificazione è soggetto ad una disciplina rigorosa ed è consentito solo previa autorizzazione di un apposito comitato istituito all'interno dell'autorità garante per la protezione dei dati personali. Una limitazione di questo tipo è consentita dalla direttiva sulla tutela dei dati ed è pertanto applicabile anche nel contesto dell'IMI.

5. Diritti delle persone cui si riferiscono i dati

5.1 Diritto all'informazione

Gli articoli 10 e 11 della direttiva sulla tutela dei dati prevedono che il responsabile del trattamento informi le persone del fatto che vengono trattati dati che li riguardano; anche il regolamento sulla tutela dei dati contiene l'obbligo di informazione. Se i dati vengono rilevati direttamente presso la persona interessata, l'articolo 10 della direttiva summenzionata prevede l'obbligo di un'informazione chiara e completa sul sistema e impone al responsabile del trattamento di informare gli interessati dell'esistenza, della finalità e del funzionamento del sistema, dei soggetti a cui verranno trasmessi i dati e del diritto di accesso, correzione e cancellazione dei dati stessi.

L'articolo 11 della medesima direttiva prevede inoltre che i responsabili del trattamento dei dati comunichino alle persone interessate se i dati che li riguardano sono raccolti presso terzi e non direttamente presso di loro. Anche in questo caso il diritto all'informazione consente di esercitare i diritti elencati in precedenza.

Per favorire il diritto all'informazione il gruppo di lavoro WP29 raccomanda di seguire una strategia d'informazione a vari livelli.

A tal fine si potrebbe ricorrere a varie misure, ad esempio una nota d'informazione indicante che tutti i dati previsti dagli articoli 10 e 11 della direttiva, ed in particolare l'identità del responsabile e la finalità del trattamento, devono essere forniti in anticipo per poter così garantire un trattamento equo dei dati.

In primo luogo la Commissione dovrebbe pubblicare sul suo sito web una nota dettagliata contenente le informazioni richieste a norma degli articoli 10 e 11 della direttiva sulla tutela dei dati e le corrispondenti disposizioni del regolamento sulla tutela dei dati; nella stessa nota dovrebbero inoltre essere descritte accuratamente le funzioni della Commissione e delle AC, con un riferimento esplicito, formulato in un linguaggio chiaro, ai diritti delle persone di cui vengono trattati i dati.

In secondo luogo ogni AC dovrebbe inserire nel proprio sito una nota riguardante la privacy, con un link alla nota sulla privacy pubblicata nel sito della Commissione.

Infine, nel sistema IMI, come in altri ambiti, le notifiche e le informazioni necessarie devono essere comunicate direttamente, individualmente e immediatamente dopo la trasmissione dei documenti da parte dei cittadini o delle AC. Tale obbligo dovrebbe essere illustrato esplicitamente a tutti i soggetti che intervengono nel sistema IMI.

5.2 Diritti di accesso, rettifica, cancellazione e blocco dei dati

L'articolo 12 della direttiva sulla tutela dei dati riguarda il diritto di accesso e rettifica: in altri termini la persona ha diritto ad accedere ai propri dati personali archiviati per verificarne l'accuratezza ed eventualmente apportarvi modifiche se sono imprecisi, incompleti od obsoleti. Il sistema IMI deve essere concepito in modo da garantire che venga rispettato il diritto di ogni individuo a consultare e rettificare i dati imprecisi, incompleti e obsoleti.

Le persone devono inoltre poter rettificare o cancellare i propri dati se il trattamento degli stessi non è conforme alla direttiva sulla tutela dei dati, in particolare per l'incompletezza o imprecisione dei dati medesimi (cfr. articolo 12, lettera b)).

Se i dati imprecisi o altri dati non validi devono essere rettificati o bloccati, il responsabile del trattamento deve informarne anche tutte le autorità competenti coinvolte nel trattamento illecito. Questa responsabilità deve essere indicata espressamente; a tal fine sarebbe estremamente utile per tutte le parti in causa disporre di un'interfaccia IMI concepita appositamente per permettere tale comunicazione. Potrebbe anche essere necessario istituire una procedura nel caso in cui i cittadini decidano di esercitare il proprio diritto alla cancellazione dei dati, per far sì che i dati vengano effettivamente eliminati da tutti i database, anche quelli esterni al sistema IMI, istituendo anche un coordinamento fra le autorità competenti.

Ogni eventuale diniego di accesso deve fondarsi su una deroga specifica prevista dal diritto nazionale in materia di protezione dei dati ed essere accuratamente motivato.

Se l'autorità interessata non risponde entro un lasso di tempo ragionevole, o non solleva obiezioni, l'autorità alla quale è stata presentata la domanda di accesso può decidere in base alla propria legislazione nazionale. Se le autorità non concordano sulla concessione dell'accesso, l'autorità che ha fornito le informazioni dovrebbe essere quella deputata ad applicare in ultima istanza i criteri in materia di accesso ai dati.

Se l'accesso è negato, occorre specificarne chiaramente i motivi e informare la persona interessata della facoltà di contattare un'altra autorità competente per accedere ai dati oppure di rivolgersi all'autorità di controllo e tutela dei dati come previsto dall'articolo 28, fatto salvo il diritto di avviare un procedimento giudiziario.

Un meccanismo di cooperazione analogo dovrebbe applicarsi anche in caso di rettifica, cancellazione o blocco dei dati.

Se una richiesta di dati viene inviata alla Commissione, quest'ultima può autorizzare l'accesso solo ai dati ai quali essa stessa può legittimamente accedere; in ogni caso, la persona interessata deve essere indirizzata verso l'autorità che ha accesso alle informazioni, nel rispetto delle garanzie introdotte dal regolamento sulla tutela dei dati

5.3 Metodi di impugnazione

Un altro elemento cruciale è dare la facoltà agli interessati di adire le vie legali se vengono violati i loro diritti. Le persone che subiscono ripercussioni negative a seguito di un trattamento improprio o illecito dei dati personali devono inoltre avere il diritto di chiedere un indennizzo per i danni subiti.

6. Sicurezza

Secondo l'articolo 17 della direttiva sulla tutela dei dati, il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati. Tali misure di sicurezza dovrebbero essere proporzionate alle finalità per le quali vengono rilevati i dati ed essere conformi alle norme in

materia di sicurezza dei singoli Stati membri. Disposizioni analoghe vengono fissate anche nel regolamento sulla tutela dei dati.

La legittimità di un sistema di trattamento dei dati che comporta rischi potenzialmente elevati dipende dalla possibilità di mantenere un livello sufficientemente elevato di sicurezza dei dati in ogni elemento che determina la funzionalità del sistema.

Inoltre, per garantire che il sistema sia sicuro per i dati particolarmente sensibili che può contenere (ad esempio quelli relativi alle sanzioni penali), secondo il WP29 è essenziale imporre l'applicazione di una serie di provvedimenti specifici, di carattere tecnico ed organizzativo, che puntino ad evitare qualsiasi alterazione, perdita, trattamento o accesso non autorizzati e a garantire la riservatezza e l'integrità delle informazioni. Questo documento non raccomanda alcun quadro o strumento tecnologico specifico per la sicurezza dei dati, ma questi criteri devono essere rispettati per tutelare adeguatamente i dati personali nel contesto dell'IMI.

Le misure di sicurezza devono essere tali da consentire di:

- evitare l'accesso al sistema da parte di persone non autorizzate;
- controllare i dati trattati, quando sono stati trattati e da chi;
- controllare l'immissione dei dati per evitare che vengano aggiunti dati o modificati quelli esistenti senza autorizzazione;
- istituire controlli sull'accesso per far sì che gli utenti accedano solo ai dati che sono autorizzati a trattare;
- controllare la comunicazione per poter determinare quali sono le autorità autorizzate a divulgare determinati dati;
- garantire la sicurezza della trasmissione per evitare l'accesso, la copia, la modifica o l'eliminazione non autorizzati dei dati nel corso dello scambio di informazioni.

Altri provvedimenti riguardano la possibilità di fare copie di riserva (*back-up*), di recuperare i dati e di procedere a test in previsione dell'applicazione del sistema utilizzando dati reali e trasmettendoli attraverso le reti di telecomunicazione criptando le informazioni o utilizzando altri meccanismi per rendere incomprensibili le informazioni o impedire che vengano manipolate da terzi.

Se la Commissione è responsabile dell'applicazione di tali misure per quanto riguarda la funzionalità e la sicurezza del server centrale, l'utilizzo sicuro delle reti è invece un elemento importante anche per gli Stati membri.

La Commissione è inoltre tenuta a rispettare le disposizioni in materia di sicurezza fissate nel regolamento sulla tutela dei dati, che devono tuttavia essere interpretate alla luce delle buone prassi esistenti negli Stati membri.

Le autorità competenti saranno tenute a conformarsi alle norme in materia di protezione dei dati vigenti nei rispettivi Stati membri e alle disposizioni riguardanti la sicurezza dei dati fissate all'articolo 17 della direttiva sulla tutela dei dati.

Inoltre, poiché la Commissione non ritiene necessario accedere ai dati personali dei lavoratori o dei prestatori di servizi migranti presenti sul server centrale, a parere del WP29 tali dati devono essere criptati per garantire la sicurezza delle comunicazioni tra le autorità competenti degli Stati membri e impedire così alla Commissione di accedere effettivamente a tali dati.

7. Notifica delle autorità di tutela dei dati e controllo preliminare

In applicazione degli articoli da 18 a 20 della direttiva sulla tutela dei dati, le organizzazioni che utilizzano il sistema IMI saranno tenute a notificare il trattamento ad almeno alcune autorità nazionali di tutela dei dati o ad essere sottoposte ad un controllo preliminare da parte loro.

Negli Stati membri che contemplano tale procedura, le operazioni di trattamento potrebbero essere soggette ad un controllo preliminare dell'autorità nazionale di tutela dei dati se tali operazioni possono presentare un rischio specifico per i diritti e le libertà delle persone interessate. Ciò potrebbe avvenire, ad esempio, se il diritto nazionale consente di trattare i dati riguardanti presunti illeciti penali solo a determinate condizioni (che di per sé potrebbero prevedere il controllo preliminare da parte dell'autorità di vigilanza nazionale competente).

Potrebbe anche accadere che l'autorità nazionale ritenga che le operazioni di trattamento possano escludere gli individui di cui si trattano i dati dall'esercizio di un diritto, dal godimento di un beneficio o da un contratto. In tal caso, sarà la legislazione nazionale e la prassi dell'autorità nazionale di tutela dei dati a decidere se tali operazioni di trattamento debbano essere sottoposte ad un controllo preliminare.

L'articolo 20 della direttiva sulla tutela dei dati prevede anche che il controllo preliminare possa avvenire durante il processo di elaborazione di un provvedimento del Parlamento nazionale, o in base ad un provvedimento fondato su tale provvedimento legislativo, in cui si definisce il tipo di trattamento e si stabiliscono appropriate garanzie.

D'altra parte, ai sensi dell'articolo 24 del regolamento sulla tutela dei dati, la Commissione europea ha nominato un responsabile della protezione dei dati personali. Le operazioni di trattamento dei dati svolte a livello della Commissione gli saranno notificate come previsto all'articolo 25 del regolamento medesimo e l'IMI sarà inserito nel registro del responsabile istituito dall'articolo 26. Considerato il ruolo che la Commissione svolge nelle operazioni di trattamento dei dati in questo caso specifico, è improbabile che sia necessario l'intervento del garante europeo della protezione dei dati (articolo 27 del regolamento).

8. Trasferimento dei dati personali a paesi terzi

Il sistema IMI non è concepito per consentire il trasferimento internazionale dei dati al di fuori della Comunità europea; la sua finalità, espressa nel mandato di cui all'articolo 34 della direttiva sui servizi, è infatti lo scambio di informazioni tra Stati membri.

Il WP29 desidera sottolineare che tali dati non devono essere trasferiti al di fuori del quadro IMI, perché i trasferimenti non rientrerebbero tra le finalità inizialmente previste per il trattamento dei dati. La trasmissione dei dati IMI verso paesi terzi costituirebbe in tal caso una violazione della limitazione all'uso dei dati sancita dall'articolo 6, paragrafo 1, lettera b), della direttiva 95/46/CE.

9. Conclusioni e raccomandazioni del WP29

1. Il sistema IMI deve essere concepito in totale conformità con i principi istituiti nelle normative applicabili in materia di protezione dei dati, tra cui la direttiva sulla tutela dei dati e il regolamento sulla tutela dei dati. I principi della protezione dei dati

devono essere applicati correttamente all’interno del sistema, perché solo così l'IMI potrà realizzare tutte le sue potenzialità e tutelare maggiormente il diritto fondamentale alla protezione dei dati personali.

2. A tale proposito, il WP29 intende sottolineare quanto sia importante rispettare le disposizioni riguardanti la qualità, la necessità e la proporzionalità dei dati ai fini della protezione degli stessi. Questi fattori devono essere considerati in tutte le fasi che caratterizzano lo sviluppo del sistema IMI e da ogni soggetto coinvolto nelle varie operazioni, dall'elaborazione di richieste d'informazione standard, alla selezione delle autorità competenti e altre ancora. Il sistema e i dati contenuti devono essere notificati alle autorità di protezione dei dati ed eventualmente essere sottoposti al loro controllo preliminare negli Stati membri che prevedono tali procedure a norma dell'articolo 18 della direttiva sulla tutela dei dati.

3. L'IMI è un sistema complesso che ha la possibilità di semplificare lo scambio delle informazioni fornendo agli Stati membri degli strumenti supplementari, ma occorre una rigorosa osservanza dei principi fissati nella direttiva sulla tutela dei dati. Gli utenti del sistema devono essere particolarmente attenti e conformarsi alle disposizioni nazionali e alla direttiva, visto che la comunicazione digitale e la possibilità di allegare documenti potenziano notevolmente le loro capacità di trasmissione delle informazioni. Ove richiesto, è inoltre necessario mantenere il ruolo di vigilanza delle autorità nazionali incaricate della tutela dei dati nonché altri controlli in vigore nei vari Stati membri. Nel contesto dell'IMI occorre infine riconoscere esplicitamente il ruolo particolare della Commissione europea descrivendo anche gli obblighi corrispondenti a tale ruolo.

4. Per permettere alle autorità competenti di utilizzare al meglio l'IMI in maniera conforme alle norme sulla protezione dei dati, occorre precisare i ruoli esattamente svolti da tutti gli utenti del sistema. È così necessario definire più accuratamente chi sono i coordinatori IMI e le autorità collegate, con i relativi diritti e responsabilità, nonché le informazioni particolari cui avranno accesso. In questo modo si potrà ridurre al minimo il trattamento superfluo dei dati, tutelando i diritti dei cittadini e del personale delle autorità competenti, senza per questo pregiudicare l'efficienza dell'IMI.

5. È importante definire con chiarezza le competenze e gli obblighi spettanti alla Commissione, ai coordinatori e alle autorità competenti, visto che i loro ruoli rispettivi nel contesto dell'IMI si possono descrivere meglio come un controllo congiunto.

6. Con lo sviluppo dell'IMI sarà necessario valutare nuovamente con attenzione le potenziali applicazioni del sistema per trasmettere dati sensibili, soprattutto nell'ambito della prima applicazione connessa alle direttive sulle qualifiche professionali e sui servizi. Tali applicazioni non sono delle possibilità astratte, visto che sono già enumerate, ad esempio all'articolo 56, paragrafo 2, della direttiva sulle qualifiche professionali, secondo il quale è possibile trasmettere informazioni penali attraverso l'IMI. Non bisogna infine dimenticare che l'IMI sarà quasi certamente utilizzato per trattare dati riguardanti la salute, gli illeciti penali o altre informazioni protette riguardanti la persona e per questo sarà imprescindibile ripensare e migliorare le misure di garanzia a fini di sicurezza e verifica.

7. Ogni singola operazione di trattamento dei dati deve imperativamente basarsi su motivazioni giuridiche individuali e legittime, adeguate alla finalità e agli obiettivi specifici del trattamento.

8. Ogni singola operazione che avviene in ambito IMI deve fondarsi su una base giuridica più concreta: ciò mette in evidente rilievo la necessità di individuare espressamente gli obiettivi delle operazioni di trattamento dei dati che avvengono nel sistema. Solo se viene specificato un obiettivo chiaro i soggetti coinvolti nell'IMI potranno avere la certezza di rispettare i principi della necessità, della qualità dei dati e della proporzionalità nel corso del loro operato. Ciascuno di questi criteri riguarda direttamente la finalità del trattamento. Anche il periodo durante il quale è possibile conservare i dati dipende da un'interpretazione specifica della finalità dell'operazione di trattamento: non è possibile sapere se un compito è stato portato a compimento se manca la certezza sul risultato auspicato. In una rete di relazioni per il trattamento dei dati così complessa come quella dell'IMI, dove può essere poco chiaro chi stia facendo cosa, è assolutamente essenziale stabilire in maniera esplicita quali sono gli obiettivi del trattamento e ottenere così un comportamento informato in situazioni incerte.
9. Il sistema IMI non potrà mai essere al servizio di 27 regimi nazionali diversi. Per questo è necessaria una decisione più specifica della Commissione, che dovrà essere precisa e finalizzata ad approfondire i punti problematici discussi in precedenza.

Fatto a Bruxelles, il 21 settembre 2007

Per il Gruppo di lavoro

Il Presidente
Peter Schaar