



1710/05/IT riv.
WP 112
04/09/12

Progetto di parere
riguardante l'attuazione del regolamento (CE n. 2252/2004 del Consiglio,
del 13 dicembre 2004, relativo alle norme sulle caratteristiche di sicurezza
e sugli elementi biometrici dei passaporti e dei documenti di viaggio
rilasciati dagli Stati membri
(Gazzetta ufficiale L 385 del 29.12.2004, pp. 1-6)

Adottato il 30 settembre 2005

Questo gruppo di lavoro è stato istituito dall'articolo 29 della direttiva 95/46/CE. Si tratta di un organo consultivo europeo indipendente, che si occupa della salvaguardia e della riservatezza dei dati. I suoi compiti sono descritti all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Alla segreteria provvede la Direzione C (Giustizia civile, diritti e cittadinanza) della Direzione generale Giustizia, libertà e sicurezza della Commissione europea, Ufficio LX-46 01/43, B-1049 Bruxelles, Belgio.

Sito web: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

Indice

Parere riguardante l'attuazione del regolamento (CE) n. 2252/2004 del Consiglio, del 13 dicembre 2004, relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri (<i>Gazzetta ufficiale L 385 del 29.12.2004, pagg. 1-6</i>)	3
1. Introduzione	3
1.1. Il problema in generale.....	3
1.2. Cronistoria e contesto del regolamento (CE) n. 2252/2004 del Consiglio.....	4
1.3. Il precedente parere del gruppo di lavoro.....	5
1.4. La risoluzione della Conferenza internazionale dei garanti della protezione dei dati e della privacy	7
2. Inserimento delle caratteristiche biometriche nei passaporti, altri documenti di viaggio e carte d'identità.....	7
2.1. Considerazioni generali.....	7
2.2. Rischi etici dell'utilizzo delle caratteristiche biometriche nei passaporti, altri documenti di viaggio e carte d'identità	8
2.3. Aspetti giuridici dell'introduzione della biometria.....	9
a) Riserve riguardo a una base centralizzata, europea o nazionale, di dati biometrici....	9
b) Accesso alla biometria solo per le autorità competenti.....	9
2.4. Aspetti tecnici.....	9
a) Inserimento dell'immagine digitalizzata del volto	10
b) Inserimento di altre caratteristiche biometriche, in particolare le impronte digitali .	11
3. Conclusioni.....	12

Parere
riguardante l'attuazione del regolamento (CE) n. 2252/2004 del Consiglio,
del 13 dicembre 2004, relativo alle norme sulle caratteristiche
di sicurezza e sugli elementi biometrici
dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri
(Gazzetta ufficiale L 385 del 29.12.2004, pp. 1-6)

**IL GRUPPO DI LAVORO PER LA TUTELA DELLE PERSONE CON RIGUARDO
AL TRATTAMENTO DEI DATI PERSONALI,**

**istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del
24 ottobre 1995¹,**

visti l'articolo 29 e l'articolo 30, paragrafo 1, lettera c) e paragrafo 3 della summenzionata direttiva,

visto il proprio regolamento interno, in particolare gli articoli 12 e 14,

HA ADOTTATO IL SEGUENTE PARERE:

1. Introduzione

1.1. Il problema in generale

Nel suo “**documento di lavoro sulla biometria**”² il gruppo di lavoro ha rilevato che i rapidi progressi della tecnologia biometrica e l'estendersi della sua applicazione negli ultimi anni richiedono un attento esame sotto il profilo della protezione dei dati. Un utilizzo ampio e incontrollato della biometria dà adito a preoccupazioni per la salvaguardia dei diritti fondamentali e della libertà personale. Questo tipo di dati è di natura speciale, poiché riguarda le caratteristiche comportamentali e fisiologiche di una persona e può consentirne l'identificazione esclusiva.

Dai tempi di queste osservazioni di base sulla biometria, si sono avuti in campo legislativo rapidi sviluppi. Il Consiglio europeo di Salonicco, del 19 e 20 giugno 2003, ha confermato che nell'Unione europea è necessaria un'impostazione coerente riguardo agli identificatori biometrici e ai dati biometrici figuranti nei documenti dei cittadini di paesi terzi, nei passaporti dei cittadini dell'Unione europea e nei sistemi d'informazione (VIS e SIS II). Nell'autunno 2003 la Commissione europea ha presentato un progetto di regolamento del Consiglio recante modifica dei regolamenti n. 1683/95 e n. 1030/2002, che istituiscono un modello uniforme rispettivamente per i visti e per i permessi di soggiorno rilasciati a cittadini di paesi terzi.

¹ Gazzetta ufficiale L 281 del 23.11.1995, pag. 31, disponibile anche in italiano sul seguente sito:
http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm

² MARKT/10595/03 – WP 80, adottato il 1° agosto 2003.

1.2. Cronistoria e contesto del regolamento (CE) n. 2252/2004 del Consiglio

Il 18 febbraio 2004 la Commissione europea ha presentato una proposta di regolamento relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici nei passaporti dei cittadini dell'Unione³. Scopo della proposta era, da un lato, rendere più sicuri i passaporti mediante uno strumento giuridicamente vincolante, riguardante le norme sulle caratteristiche armonizzate di sicurezza e, d'altro lato, stabilire un nesso sicuro tra il titolare legittimo e il documento, mediante identificatori biometrici. In tal modo, si sarebbe inoltre consentito agli Stati membri dell'UE di soddisfare alle prescrizioni del Visa Waiver Programme (programma d'esenzione dall'obbligo del visto) degli USA, nel rispetto delle norme internazionali. Nella sua proposta, la Commissione europea prevedeva che nei passaporti e altri documenti di viaggio s'includesse a titolo obbligatorio un supporto di memorizzazione, contenente l'immagine del volto. Agli Stati membri era consentito includere nei passaporti, mediante legge nazionale, le impronte digitali. La Commissione europea aveva pure proposto che l'identificatore biometrico fosse memorizzato in un supporto avente la capacità sufficiente: poteva trattarsi di un microprocessore del tipo senza contatto, ma anche di un altro supporto di memorizzazione avente la necessaria capacità. I particolari al riguardo dovevano essere decisi dagli esperti tecnici, all'interno del comitato responsabile. La proposta di regolamento offriva anche la possibilità di memorizzare le impronte digitali in una base dati nazionale, nella prospettiva di un futuro registro europeo dei documenti rilasciati.

Nell'estate 2004 la proposta è stata discussa presso il gruppo di lavoro sui visti. Infine, il 6 ottobre 2004 il CSIFA (Comitato strategico sull'immigrazione, le frontiere e l'asilo) ha discusso la proposta e l'ha trasmessa al Parlamento europeo. La proposta definitiva prevedeva l'immagine del volto come prima caratteristica biometrica a titolo obbligatorio e le impronte digitali come seconda caratteristica biometrica a titolo facoltativo.

In seguito al Consiglio GAI (Giustizia e affari interni) del 25-26 ottobre 2004, il testo della proposta è stato modificato, in modo da prevedere a titolo obbligatorio entrambe le caratteristiche biometriche⁴.

Il 2 dicembre 2004 il Parlamento europeo ha adottato con 471 voti favorevoli, 118 contrari e 6 astensioni una risoluzione legislativa, non vincolante, riguardante la proposta della Commissione di regolamento del Consiglio relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici nei passaporti dei cittadini dell'Unione⁵. Il Parlamento è favorevole all'introduzione di passaporti con l'immagine del volto, poiché questo elemento biometrico renderà più difficile falsificarli. Secondo il Parlamento, i dati biometrici assicureranno che la persona che presenta il passaporto è davvero la persona alla quale il passaporto è stato rilasciato inizialmente. Poiché il Parlamento europeo sostiene che l'inserimento degli elementi biometrici non deve violare i diritti di privacy e di protezione dei dati, esso ha rifiutato l'inserimento obbligatorio delle impronte digitali e l'istituzione di una banca dati centrale per i passaporti e documenti di viaggio dell'Unione europea. In tale risoluzione legislativa del 2 dicembre 2004 si dichiara che gli elementi biometrici figuranti

³ COM(2004)116 def., menzionata nella Gazzetta ufficiale n. C 98 del 23.4.2004, pag. 39.

⁴ Documento 15139/2004 del Consiglio.

⁵ Risoluzione legislativa del Parlamento europeo sulla proposta della Commissione di regolamento del Consiglio relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici nei passaporti dei cittadini dell'Unione (COM(2004)0116 – C5-0101/2004 – 2004/0039(CNS)), <http://www2.europarl.eu.int/omk/sipade2?PUBREF=-//EP//TEXT+TA+P6-TA-2004-0073+0+DOC+XML+V0//EN&LEVEL=2&NAV=X>.

nei passaporti vanno utilizzati soltanto per accertare l'autenticità del documento e l'identità del titolare e che devono essere memorizzati in "un supporto di memorizzazione altamente protetto, dotato di capacità sufficiente e atto a salvaguardare l'integrità, l'autenticità e la riservatezza dei dati memorizzati". Nella risoluzione è anche indicato che potranno avere accesso a tale supporto soltanto le autorità degli Stati membri competenti per leggere, memorizzare, modificare e cancellare dati biometrici. Inoltre, il Parlamento introduce un emendamento nel testo della proposta di regolamento, stabilendo esplicitamente che "non va istituita alcuna banca dati centrale per i passaporti e i documenti di viaggio dell'Unione europea che contenga i dati biometrici e di altro tipo di tutti i titolari di passaporto dell'UE". Secondo la relazione del 25 ottobre 2004 della Commissione per le libertà civili, la giustizia e gli affari interni, "la creazione di una base di dati centralizzata violerebbe la finalità e il principio di proporzionalità, aumentando peraltro il rischio di abusi e di "function creep" (incrocio indebito dei dati). Inoltre, aumenterebbe anche il rischio che si usino gli identificatori biometrici come "chiavi d'accesso" a varie banche di dati, interconnettendo in tal modo serie di dati."

Il 13 dicembre 2004 il Consiglio ha adottato il regolamento (CE) n. 2252/2004 relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri, basato sul progetto del Consiglio GAI del 25-26 ottobre 2004⁶. Tale regolamento prevede a titolo obbligatorio l'immagine digitalizzata del volto come prima caratteristica biometrica e, come seconda caratteristica biometrica, le impronte digitali, anch'esse a titolo obbligatorio. Il Consiglio non ha tenuto conto dei suggerimenti e delle richieste di emendamenti presentati dal Parlamento. A norma del suo articolo 6, il regolamento è entrato in vigore il 18 gennaio 2005. Nel medesimo articolo 6, il regolamento stabilisce che gli Stati membri l'applicheranno:

"a) per quanto riguarda l'immagine del volto: al più tardi 18 mesi

b) per quanto riguarda le impronte digitali: al più tardi 36 mesi

dall'adozione delle misure di cui all'articolo 2."

Il 28 febbraio 2005 la Commissione europea ha approvato la "Decisione volta a stabilire le specifiche tecniche relative alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri"⁷, che si riferisce all'articolo 2 del regolamento (CE) n. 2252/2004 del Consiglio.

1.3. Il precedente parere del gruppo di lavoro

Il 18 agosto 2004 il presidente del gruppo di lavoro articolo 29 aveva inviato una lettera al presidente del Parlamento europeo, al presidente della commissione LIBE, al segretario generale del Consiglio dell'Unione europea, al presidente della Commissione europea, al direttore generale della DG Imprese e al direttore generale della DG Giustizia e affari interni, presentando loro le seguenti proposte concrete⁸:

⁶ GU L 385 del 29.12.2004, pagg. 1-6.

⁷ C(2005) 409 def. (non ancora pubblicata nella Gazzetta ufficiale).

⁸ Lettera del presidente del gruppo di lavoro articolo 29 al presidente del Parlamento europeo, al presidente della commissione LIBE, al segretario generale del Consiglio dell'Unione europea, al presidente della

1. Il gruppo di lavoro si opponeva strenuamente alla memorizzazione dei dati biometrici e di altro tipo di tutti i titolari di un passaporto UE in una base di dati centralizzata dei passaporti e documenti di viaggio europei.
2. Lo scopo d'introdurre le caratteristiche biometriche nei passaporti e documenti di viaggio, da definire nel regolamento, doveva essere esplicito, adeguato, proporzionato e chiaro.
3. Gli Stati membri dovevano garantire secondo modalità tecnicamente valide che nei passaporti fosse inserito un supporto di memorizzazione dotato di capacità sufficiente e atto ad assicurare la completezza, l'autenticità e la riservatezza dei dati.
4. Nel regolamento si doveva stabilire chi potrà accedere al supporto di memorizzazione ed a quali scopi (leggere, memorizzare, modificare o cancellare dati).
5. Gli Stati membri dovevano istituire un registro delle autorità competenti.

Il presidente faceva notare che le caratteristiche di sicurezza nei passaporti e documenti di viaggio dovevano essere valide e garantite per l'intero periodo di validità del documento. La responsabilità delle norme di sicurezza e delle necessarie infrastrutture spetta alle autorità che rilasciano tali documenti. Non si possono biasimare i cittadini per gli errori che si commettono in questo campo quando viene preparato e rilasciato il documento o nel corso del suo periodo di validità.

Infine, il presidente richiamava l'attenzione sul parere riguardante la biometria (WP 80), adottato dal gruppo di lavoro il 1° agosto 2003⁹ e sul parere riguardante le caratteristiche biometriche nei visti e permessi di soggiorno (WP 96), adottato l'11 agosto 2004¹⁰.

In un'altra lettera inviata il 30 novembre 2004 al presidente della commissione LIBE e al presidente del Consiglio dell'Unione europea, il presidente del gruppo di lavoro articolo 29 presentava argomentazioni contro la seconda caratteristica biometrica obbligatoria, sostenendo che introducendola sarebbe stato tanto più necessario istituire un sistema sicuro a tutta prova, per evitare di ledere il diritto fondamentale alla privacy.

A tale riguardo, si deve tener conto anche del recente parere del gruppo di lavoro articolo 29 (WP110), del 23 giugno 2005, sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (COM (2004) 835 def.)¹¹. In tale parere si rammenta la posizione del gruppo di lavoro articolo 29 sulla biometria e si chiede d'istituire adeguate salvaguardie per il trattamento dei dati biometrici nel VIS.

Commissione europea, al direttore generale della DG Imprese e al direttore generale della DG Giustizia e affari interni, in data 18 agosto 2004 (non pubblicata).

⁹ MARKT/10595/03/EN – WP 80, adottato il 1° agosto 2003.

¹⁰ MARKT/11224/04/EN – WP 96, adottato l'11 agosto 2004.

¹¹ MARKT/1022/05/EN.

1.4. La risoluzione della Conferenza internazionale dei garanti della protezione dei dati e della privacy

Il 16 settembre 2005, la 27^a Conferenza internazionale dei garanti della protezione dei dati e della privacy, svoltasi a Montreux, ha adottato una **risoluzione sull'utilizzo della biometria nei passaporti, carte d'identità e documenti di viaggio**¹². In tale risoluzione, la Conferenza internazionale osserva che il diffuso utilizzo della biometria avrà effetti a lungo raggio sulla società globale e deve quindi formare oggetto di un ampio dibattito a livello mondiale. La Conferenza internazionale chiede che:

1. si predispongano tempestivamente efficaci garanzie, per limitare i rischi inerenti alla natura della biometria;
2. si tengano rigorosamente distinti i dati biometrici raccolti e memorizzati rispettivamente in base ad obblighi di legge, per scopi di natura pubblica (per esempio i controlli alle frontiere) e in base al consenso, per scopi contrattuali;
3. si applichino restrizioni tecniche all'utilizzo della biometria nei passaporti e carte d'identità ai fini della verifica, tramite il confronto fra i dati contenuti nel documento e i dati forniti dal detentore che lo presenta.

2. Inserimento delle caratteristiche biometriche nei passaporti, altri documenti di viaggio e carte d'identità

L'articolo 1, paragrafo 2 del regolamento (CE) n. 2252/2004 prevede a titolo obbligatorio l'inserimento dell'immagine digitalizzata del volto e delle impronte digitali, quali caratteristiche biometriche, nei passaporti dei cittadini UE. A norma dell'articolo 6 e secondo la decisione C(2005) 409 della Commissione europea, del 28 febbraio 2005, gli Stati membri dovranno inserire nei passaporti dei loro cittadini l'immagine digitalizzata del volto entro il 28 agosto 2006 e le impronte digitali entro il 28 febbraio 2008. I primi Stati membri dovevano cominciare già nell'autunno 2005 a rilasciare i cosiddetti passaporti elettronici, con l'immagine digitalizzata del volto memorizzata in un chip RFID. Negli Stati membri che rilasciano carte d'identità si sta pensando d'introdurvi le caratteristiche biometriche.

2.1. Considerazioni generali

L'inserimento delle caratteristiche biometriche nei passaporti avrà conseguenze a lungo raggio per i detentori di passaporti: di conseguenza, non è possibile procedervi senza un'adeguata valutazione dei suoi effetti sulla privacy. Sinora bastava avere nei passaporti o altri documenti di viaggio la descrizione di alcune caratteristiche biometriche: la fotografia, l'indicazione del sesso, della statura o del colore degli occhi. Dopo l'attuazione del regolamento (CE) n. 2252/2004 del Consiglio, i cittadini europei dovranno fornire dati biometrici in forma digitalizzata. Questi dati possono esser memorizzati in basi di dati e resi disponibili per tutta una serie di scopi imprevedibili.

¹² <http://www.privacyconference2005.org> (non ancora pubblicata). NdT: Traduzioni italiane non ufficiali si trovano in Internet, per esempio all'indirizzo <http://www.privacy.it/garantemont2005-biometria.html>.

2.2. Rischi etici dell'utilizzo delle caratteristiche biometriche nei passaporti, altri documenti di viaggio e carte d'identità

Sono numerosi i rischi etici inerenti all'inserimento delle caratteristiche biometriche nei passaporti, altri documenti di viaggio e carte d'identità. Nell'ottobre 2004, nell'ambito del sesto programma quadro in materia di ricerca e sviluppo tecnologico (FP6) è stato varato il progetto BITE ("Biometric Identification Technology Ethics": etica della tecnologia d'identificazione biometrica)¹³, finanziato dalle Comunità europee. Gli obiettivi del BITE sono stimolare la ricerca e lanciare un pubblico dibattito sulla bioetica nella tecnologia biometrica. Nel giugno 2006 si procederà alla consultazione del pubblico. Un altro progetto sostenuto dall'Unione europea nell'ambito dell'FP6 è il FIDIS¹⁴ ("Future of Identity in the Information Society": il futuro dell'identità nella società dell'informazione), che è attuato da un consorzio di università e imprese europee, con la partecipazione di altri istituti pubblici e privati. Scopo del FIDIS è configurare le esigenze della futura gestione dell'identità nella società europea dell'informazione e contribuire alle tecnologie e infrastrutture necessarie¹⁵.

Secondo uno studio prospettico¹⁶ fatto redigere dalla commissione LIBE del Parlamento europeo, si dovrebbe disporre di procedure di ripiego tali da costituire garanzie essenziali per l'inserimento dei dati biometrici, poiché essi non sono né accessibili a tutti né completamente esatti. Simili procedure dovrebbero essere attuate e utilizzate in modo da rispettare la dignità delle persone che non possano compiere con esito positivo il processo di registrazione e da evitare d'imputar loro le imperfezioni del sistema¹⁷

Uno degli aspetti del dibattito riguarda il fatto che le istituzioni governative e altre pubbliche autorità saranno in grado di raccogliere e memorizzare un grandissimo numero d'informazioni delicate sui loro cittadini. In tale contesto, si deve osservare in particolare che raccogliere caratteristiche biometriche significa raccogliere dati relativi al *corpo* di una persona.

Un altro aspetto è che sinora si sono raccolte caratteristiche biometriche, come le impronte digitali, perlopiù in caso di fatti delittuosi. L'interrogativo è: i cittadini europei saranno disposti a farsi prendere le impronte digitali per altri scopi?

Altre preoccupazioni sono di natura differente. Le persone la cui identità è più difficile da comprovare, per esempio gli immigranti, possono trovarsi ingiustamente ad essere le vittime in un simile sistema. Le persone disabili che non sono in grado di sottoporsi a test biometrici possono subire un danno morale, e a loro riguardo si possono raccogliere dati medici di natura delicata. A livello pratico, le leggi in materia di privacy sono diverse nei vari paesi, il che ha ripercussioni sulla trasmissione reciproca dei dati e sull'interrelazione tra le basi di dati.

¹³ <http://www.biteproject.org/>

¹⁴ <http://www.fidis.net>

¹⁵ Altri due progetti, BIOSEC e BIOSECURE, pure finanziati dall'FP6, esaminano in certa misura anch'essi tale questione. <http://www.biosec.org> and <http://www.biosecure.info>

¹⁶ Istituto di prospettiva tecnologica (Commissione europea, DG Centro comune di ricerca), "Biometrics at the Frontiers: Assessing the Impact on Society" (La biometria alle frontiere: valutazione del suo impatto sociale), febbraio 2005.

¹⁷ Consiglio d'Europa: "Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data" (Relazione riguardante i progressi nell'applicazione dei principi della Convenzione 108 alla raccolta e all'elaborazione di dati biometrici), 2005, pag. 11.

Quando si tratta di memorizzare impronte digitali, si deve fare attenzione alle varie correlazioni, di cui si discute attualmente, tra le impronte palmari e determinate malattie. Si dice per esempio che certe caratteristiche del palmo della mano e dei polpastrelli sono correlate con la nutrizione della madre (e quindi del feto) nel terzo mese di gravidanza¹⁸. La leucemia e il cancro al seno sembrano correlati statisticamente a certe caratteristiche palmari. Sono ignote le correlazioni precise o dirette in questi casi, ma a tale riguardo si svolgono attualmente dibattiti scientifici che non si possono ignorare.

2.3. Aspetti giuridici dell'introduzione della biometria

a) Riserve riguardo a una base centralizzata, europea o nazionale, di dati biometrici

Nella risoluzione legislativa del 2 dicembre 2004 il Parlamento europeo ha chiesto che si vieti l'istituzione di una base centrale dei passaporti e documenti di viaggio dell'Unione europea contenente i dati biometrici e di altra natura di tutti i titolari di un passaporto UE. Il gruppo di lavoro appoggia tale richiesta e dichiara che le obiezioni contro una simile base centrale europea dei passaporti e documenti di viaggio dell'Unione europea coincidono con le obiezioni contro le basi centrali nazionali di dati dei passaporti e documenti di viaggio e delle basi centrali di dati delle carte d'identità.

Vi è il rischio che, istituendo una banca centralizzata di dati comprendente i dati personali e in particolare i dati biometrici di tutti i cittadini (europei), si possa violare il principio basilare della proporzionalità. Ogni base centrale di dati accrescerebbe i rischi di utilizzo improprio e di appropriazione indebita, aggraverebbe i pericoli di abuso e d'incrocio indebito di dati e aumenterebbe anche le possibilità di utilizzare gli identificatori biometrici come "chiavi di accesso" a varie basi di dati, stabilendo interconnessioni tra serie di dati.

b) Accesso alla biometria solo per le autorità competenti

Le caratteristiche biometriche nei passaporti, in tutti gli altri documenti di viaggio o nelle carte d'identità, sono di natura molto delicata. Si deve quindi assicurare che soltanto le autorità competenti possano avere accesso ai dati memorizzati nel chip. Non si potrà ammettere un accesso non autorizzato. A tale scopo, il gruppo di lavoro sostiene la richiesta del Parlamento europeo, secondo cui ogni Stato membro dovrà tenere un registro delle autorità competenti e degli organismi autorizzati di cui all'articolo 3 del regolamento (CE) n. 2252/2004. Gli Stati membri trasmetteranno tale registro e, se necessario, i successivi aggiornamenti alla Commissione, che terrà un registro aggiornato on line e pubblicherà ogni anno tutta la serie dei registri nazionali.

In caso di rifiuto ai controlli di frontiera o nel corso di altri controlli effettuati dalle autorità competenti, gli interessati devono essere informati dei motivi del rifiuto, di quali mezzi dispongono per far valere il proprio punto di vista ed a quali autorità devono presentare ricorso.

2.4. Aspetti tecnici

I rischi di natura tecnica sono di vario tipo: riguardano l'introduzione del chip senza contatto (chip RFID) e l'inserimento delle caratteristiche biometriche nel chip.

¹⁸ FIDIS: "Study on PKI and biometrics" (Studio sulla PKI e la biometria), pag. 68.

Nella risoluzione legislativa del 2 dicembre 2004, il Parlamento europeo ha chiesto che i passaporti comprendano un supporto di memorizzazione ad alto grado di sicurezza, dotato di capacità sufficiente e tale da salvaguardare l'integrità, l'autenticità e la riservatezza dei dati memorizzati. Il gruppo di lavoro si è dichiarato favorevole a tale richiesta¹⁹, di cui tuttavia il Consiglio non ha tenuto conto. Il chip RFID (norma ISO 14443), che è previsto nel regolamento del 13 dicembre 2004, fa sorgere tutta una serie di rischi per il diritto alla privacy dei cittadini europei. La decisione della Commissione del 28 febbraio 2005²⁰ non è atta a tutelare i diritti dei cittadini, poiché il contatto tra il chip RFID e il lettore si presta all'intercettazione ("eavesdropping") e le informazioni possono essere captate e copiate ("skimming").

I rischi derivanti dall'introduzione del chip RFID nei passaporti, in altri documenti di viaggio o nelle carte d'identità e dall'inserimento delle caratteristiche biometriche nel chip richiedono una struttura di sicurezza volta ad assicurare un maggior livello di riservatezza per le informazioni da scambiare. Il gruppo di lavoro, che si rende ben conto di tali problemi, ritiene necessaria un'infrastruttura globale a chiave pubblica (PKI). I certificati a chiave pubblica contengono informazioni sul titolare e ognuno di essi rimanda unicamente alla persona alla quale è stato rilasciato: i certificati digitali sono unici, come il numero delle carte di credito e il numero di affiliazione ai regimi di prestazioni sociali e di assistenza sanitaria. Tuttavia, i certificati digitali si prestano a un utilizzo indebito, inteso a negare al titolare del certificato l'accesso ai servizi. Inoltre, i dati generali dell'operazione svolta mediante certificati digitali può essere filtrata da strumenti di sorveglianza ed essere trasmessa elettronicamente a terzi o alla polizia o altre autorità.

In considerazione di tali rischi, è imperativo creare un profilo di protezione (PP) rispondente ai criteri comuni per la valutazione della sicurezza della tecnologia dell'informazione ("Common Criteria", CC), vers. 2.1 (norma ISO 15408), i quali forniscono una soluzione generalmente accettata per i problemi di sicurezza della TI. Il profilo di protezione, che descrive un concetto di sicurezza TI che deve essere completo, costante e coerente, deve essere presentato dal comitato istituito dall'articolo 5 del regolamento (CE) n. 2252/2004. Secondo gli emendamenti proposti dal Parlamento europeo nella risoluzione legislativa del 2 dicembre 2004, il gruppo di lavoro suggerisce che il comitato sia coadiuvato da esperti scelti dal gruppo stesso.

a) Inserimento dell'immagine digitalizzata del volto

Secondo la decisione della Commissione europea del 28 febbraio 2005, gli Stati membri sono tenuti a introdurre nei passaporti dei loro cittadini l'immagine digitalizzata del volto entro il 28 agosto 2006. In applicazione dell'articolo 1 e del punto 5.2 dell'allegato della decisione, gli Stati membri devono assicurare l'accesso ai dati contenuti nel chip mediante un dispositivo di sicurezza denominato controllo di base dell'accesso (Basic Access Control, BAC). Il BAC è raccomandato dall'Organizzazione internazionale dell'aviazione civile

¹⁹ Lettera del presidente del gruppo di lavoro articolo 29 al presidente del Parlamento europeo, al presidente della commissione LIBE, al segretario generale del Consiglio dell'Unione europea, al presidente della Commissione europea, al direttore generale della DG Imprese e al direttore generale della DG Giustizia e affari interni, in data 18 agosto 2004 (non pubblicata).

²⁰ C(2005) 409 def.

(ICAO), ma non è obbligatorio²¹. Il suo scopo è prevenire lo skimming e l'eavesdropping, garantendo che l'accesso ai dati, in particolare quelli biometrici, sia possibile soltanto quando, prima di leggere i dati del chip, un contatto ottico tra il passaporto e il dispositivo di lettura abbia costituito una chiave di accesso di base al documento ("Document Basic Access Key"), dalla zona a lettura ottica ("machine readable zone", MRZ) del passaporto. La chiave di accesso di base al documento viene elaborata tenendo conto del numero del passaporto, la sua data di scadenza e la data di nascita del titolare. Una volta costituita la chiave di accesso di base al documento, il dispositivo di lettura è in grado di leggere i dati memorizzati nel chip RFID. Ai fini della sicurezza, i dati vengono trasmessi in forma cifrata, il che implica un chip a sicurezza certificata, comprendente un coprocessore cifrato²².

Tuttavia, il BAC non costituisce un dispositivo adeguato di sicurezza: esso si basa sull'MRZ del passaporto, ma questi dati non sono trattati con rigorosa riservatezza. Per esempio, se un cittadino europeo vuole procurarsi un biglietto per un evento speciale, quale la Coppa del mondo FIFA 2006 in Germania o il campionato europeo UEFA 2008 in Austria e in Svizzera, deve indicare su un modulo internet nome e cognome, data di nascita, numero del passaporto o della carta d'identità e il giorno di rilascio del documento. Si è applicata questa procedura già per la vendita dei biglietti per il campionato europeo UEFA 2004 in Portogallo e la si applicherà ancora per qualche altro evento, come concerti o altre grandi manifestazioni sportive, quali le Olimpiadi o i campionati mondiali di atletica. Poiché in alcuni Stati membri le agenzie private copiano i passaporti o carte d'identità a titolo di garanzia del loro credito, le parti costitutive della chiave di accesso di base al documento non sono segrete e c'è da temere che l'algoritmo del BAC finirà per essere disponibile su internet.

b) Inserimento di altre caratteristiche biometriche, in particolare le impronte digitali

Le circostanze nelle quali si procede a prelevare le impronte digitali dovranno garantire affidabilità perfetta. L'ICAO, che non considera una questione delicata l'immagine digitalizzata del volto, poiché sui passaporti vi è la fotografia del titolare, riconosce invece che inserire nei passaporti le impronte digitali e altre caratteristiche biometriche è qualcosa di estremamente delicato. L'ICAO raccomanda quindi uno speciale dispositivo di sicurezza, denominato controllo esteso dell'accesso (Extended Access Control, EAC)²³, il cui funzionamento è analogo a quello, già descritto, del BAC. Tuttavia, per questo controllo esteso si utilizzano una serie di chiavi di accesso esteso al documento, invece delle chiavi dell'accesso di base. Questa serie di chiavi (unica per ogni chip), che viene determinata dallo Stato che rilascia il documento, può consistere in chiavi simmetriche, derivanti per esempio dall'MRZ e da una chiave universale nazionale, oppure in una coppia di chiavi asimmetriche, con una carta certificato corrispondente. Nondimeno, numerosi particolari di tali dispositivi di sicurezza sono tuttora da chiarire.

²¹ ICAO: "Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access" (Relazione tecnica: la PKI per i documenti di viaggio a lettura ottica ad accesso per sola lettura ICC), versione 1.1, pubblicata il 1° ottobre 2004, pag. 16.

²² Allo scopo della sicurezza di trasmissione, il cosiddetto gruppo Essen ha sviluppato un software speciale, denominato "Golden Reader Tool" (strumento d'oro di lettura). Il gruppo Essen comprende pubbliche autorità, imprese del settore della sicurezza TI e imprese che producono documenti di viaggio di Germania, Paesi Bassi e Regno Unito.

²³ ICAO: "Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access" (Relazione tecnica: la PKI per i documenti di viaggio a lettura ottica ad accesso per sola lettura ICC), versione 1.1, pubblicata il 1° ottobre 2004, pag. 17.

Il controllo esteso dell'accesso costituisce un progresso per quanto riguarda le misure di sicurezza, ma tale dispositivo è solo opzionale, come lo è il BAC²⁴. Si aggiunga che non è affatto sicuro che l'EAC sarà applicato dagli Stati non membri. La Commissione europea e gli Stati membri devono garantire che i passaporti dei cittadini europei comprendenti le impronte digitali non possano essere letti da lettori non in grado di supportare il controllo esteso dell'accesso.

3. Conclusioni

L'inserimento delle caratteristiche biometriche nei passaporti, altri documenti di viaggio e carte d'identità solleva numerosi problemi etici, giuridici e tecnici. Di conseguenza, il gruppo di lavoro richiama l'attenzione sui seguenti aspetti:

1. Prima d'introdurre le caratteristiche biometriche nei passaporti, altri documenti di viaggio e carte d'identità, deve svolgersi un esauriente dibattito sociale. A tale scopo, è necessario attendere i risultati del progetto BITE.
2. Per limitare i rischi inerenti alla natura della biometria, si devono applicare tempestivamente garanzie efficaci. A tal scopo, il comitato istituito dall'articolo 5 del regolamento (CE) n. 2252/2004, che dovrà essere coadiuvato da esperti scelti dal gruppo di lavoro articolo 29, dovrà presentare un profilo di protezione.
3. Si deve garantire la rigorosa distinzione tra i dati biometrici raccolti e memorizzati rispettivamente per scopi pubblici (per esempio ai controlli di frontiera), in base ad obblighi di legge, e per scopi contrattuali, in base a consenso.
4. L'impiego della biometria nei passaporti e carte d'identità va limitato con mezzi tecnici ai soli scopi di verifica, per comparare i dati inclusi nel documento con i dati forniti dal detentore quando presenta tale documento.
5. La Commissione europea e gli Stati membri devono assicurare che i passaporti di cittadini europei comprendenti le impronte digitali non possano essere letti da lettori non in grado di supportare il controllo esteso dell'accesso.
6. Si deve assicurare che soltanto le autorità competenti possano avere accesso ai dati memorizzati nel chip. Gli Stati membri istituiranno un registro delle autorità competenti.

Bruxelles, 30 settembre 2005

Per il gruppo di lavoro
Il Presidente
Peter Schar

²⁴ ICAO: "Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access" (Relazione tecnica: la PKI per i documenti di viaggio a lettura ottica ad accesso per sola lettura ICC), versione 1.1, pubblicata il 1° ottobre 2004, pagg 17, 21 e 22.

