

Il Garante ha di recente indicato il permesso di soggiorno elettronico quale possibile strumento utile nel rispetto delle regole sulla sicurezza, confermando, di fatto, quanto emerge ormai indiscutibilmente in ogni settore della vita dell'individuo, e cioè come il buon uso dello strumento elettronico nella varietà e nella fantasia delle soluzioni proposte ne diviene importante componente.

di Francesca Panuccio Dattola

PERMESSO DI SOGGIORNO ELETTRONICO: VIA LIBERA DEL GARANTE ALLE REGOLE DI SICUREZZA

Francesca PANUCCIO DATTOLA, avvocatessa esperta in diritto di famiglia, professore associato e titolare di cattedra di Diritto dell'informatica, presso la Università di Messina, dipartimento di Diritto privato. Insegna informatica giuridica presso la medesima università e presso le scuole di specializzazione per la professione forense di Messina e Palermo (LUMSA).



Il provvedimento del Garante, ultimo in ordine di tempo, del 5 marzo 2015 n. 119, emesso a seguito della richiesta del Ministero dell'Interno in ordine a "procedure e processi di produzione e di servizio per il procedimento di emissione e controllo del permesso di soggiorno" consente di ripercorrere le tappe principali che hanno portato il Garante oggi ad indicare il permesso di soggiorno elettronico quale possibile strumento utile nel rispetto delle regole sulla sicurezza. Si conferma così quanto emerge ormai indiscutibilmente in ogni settore della vita dell'individuo, e cioè come il buon uso dello strumento elettronico nella varietà e nella fantasia delle soluzioni proposte ne diviene importante componente. E infatti con provvedimento del 05/03/2015 il Garante della Privacy ha evidenziato come il diritto di protezione dei dati personali, attraverso l'indicazione dallo stesso fornita per elevare il livello delle garanzie per gli interessati - recepita dall'Amministrazione - consenta di esprimere parere positivo sullo schema di decreto direttoriale proposto. La struttura del parere - essenziale nelle argomentazioni proposte - riprende la definizione tecnica del permesso di soggiorno, costituito da un supporto fisico (tessera o *smartcard*) con gli elementi e i requisiti di sicurezza previsti dalle prescrizioni tecniche stabilite nell'Allegato I alla Decisione C(2009) 3770 (classificato "SECRET UE"), nonché da un microprocessore RF integrato contenente i dati del permesso di soggiorno, in conformità al Regolamento CE n. 380/2008 e alle prescrizioni tecniche stabilite nell'allegato II alla Decisione della Commissione C(2009) 3770 del 20 maggio 2009. Il PES introdotto nel dicembre del 2006¹ è costituito da una *smartcard* su cui sono stampati i dati e la fotografia del titolare, e nella quale è inserito un microprocessore con i dati identificativi dell'intestatario, tra cui l'immagine del volto e le impronte digitali. Per garantire un elevato livello di sicurezza, il circuito di emissione e controllo del permesso si basa su un'architettura centralizzata che consente sia la tracciatura di tutte le operazioni effettuate da ciascun ente coinvolto, sia l'emissione di documenti in grado di minimizzare i rischi di contraffazione e falsificazione². I tre schemi, sottoposti al giudizio dell'Autorità, individuano le prescrizioni tecniche relative alle procedure e ai processi di produzione per l'emissione e il controllo del permesso di soggiorno.

Il permesso di soggiorno, come è noto, è l'autorizzazione rilasciata dalle autorità di uno Stato membro che consente ad un cittadino di un paese terzo³ di soggiornare legalmente nel proprio territorio, definizione che si ricava dal Regolamento CE del Consiglio 13/06/2002 n. 1030/2002, che ha introdotto un modello uniforme (*Modèle uniforme de permis del séjour*) per i permessi di soggiorno rilasciati a cittadini terzi, al fine di creare un documento che contenga tutte le informazioni necessarie e soddisfi elevati requisiti tecnici in particolare per quanto attiene alle garanzie contro la contraffazione e la falsificazione. Oggi il Regolamento CE n. 380 del 2008 ha modificato il Regolamento CE n. 1030/2002. Nel D.Lgs. 286/1998 novellato dal nuovo comma 2-bis si prescriveva la necessità di prendere i rilievi foto dattiloscopici, per ogni straniero che richiedeva il permesso di soggiorno o il rinnovo, mentre il D.Lgs. n. 394 del 1999 all'art. 9 consentiva agli addetti della questura di richiedere allo straniero in luogo delle fotografie di farsi ritrarre da apposita apparecchiatura per il trattamento automatizzato dell'immagine. L'obiettivo era e rimane quello di raggiungere una certezza sull'identità dello straniero, anche al fine di fermare persone sospette prima dell'entrata nel Paese. Non si può infatti dimenticare che i terroristi e i criminali tentano di infiltrarsi usando nomi fittizi e falsi passaporti. Si tratta allora oggi di verificare se nel permesso di soggiorno elettronico, attraverso le regole tecniche contenute nei tre decreti ed approvate dal Garante, si ritrovano e in che misura le medesime garanzie di sicurezza e di protezione dei dati personali previste nei decreti richiamati. Dal punto di vista strutturale è corretto affermare che il documento elettronico, simile ad un bancomat, sarà dotato di un microprocessore *contactless* (ICs) con tecnologia a radiofrequenze e pertanto il livello di rispondenza alla identità della persona è raggiunto. Nel supporto informatico di memorizzazione verranno raccolti, tra gli altri: i dati personali del richiedente o titolare del permesso di soggiorno, i dati identificativi del documento, gli elementi biometrici primari (immagine del volto) e quelli secondari (impronte digitali). Le persone che ottengono il permesso di soggiorno elettronico secondo le nuove regole, saranno fornite di una tessera dotata di microprocessore *contactless* contenente le informazioni necessarie per verificare l'autenticità del documento, nonché i dati identificativi, la fotografia e le impronte digitali del titolare. A garanzia del trattamento dei dati della persona, le

regole prevedono che il microprocessore potrà essere letto esclusivamente dagli organi di controllo e solo per verificare l'identità del titolare e l'autenticità del documento stesso. La decisione del Garante contiene poi una sottolineatura circa le fasi del procedimento di emissione del PSE che diventa rafforzamento della protezione dei dati della persona. In particolare: pianificazione dei bisogni e produzione dei supporti dei permessi di soggiorno; gestione delle richieste di rilasci dei permessi di soggiorno previa acquisizione elettronica dell'istanza di richiesta di rilascio del permesso di soggiorno da parte dell'IPZS; spedizione, trasporto e presa in carico dei permessi di soggiorno da parte dell'Ufficio immigrazione e consegna del permesso di soggiorno allo straniero da parte dell'Ufficio. Nell'ambito della fase di gestione delle istanze di rilascio del PSE di particolare importanza per la protezione dei dati personali assume la già ricordata procedura per l'assunzione dei rilievi dattiloscopici, fase necessaria per l'identificazione dello straniero. La acquisizione del riferimento univoco della pratica per la successiva associazione al cartellino fotosegnalatico; lo svolgimento dei rilievi foto dattiloscopici e la generazione di un codice identificativo (CUI); la trasmissione dello stesso CUI e il numero univoco della pratica all'infrastruttura Centrale, coniugano insieme esigenze di sicurezza e di riferibilità alla persona, in maniera da ridurre le ipotesi di errore, anzi escludendole del tutto. Importante diventa poi la formazione di un archivio immigrazione con le connesse qualità e responsabilità per la protezione dei dati personali. Si tratta di trattamenti che prevedono la realizzazione di archivi biometrici centralizzati, per i quali continua ad essere obbligatorio richiedere una verifica preliminare ai sensi dell'art. 17 del Codice privacy. I dati biometrici dell'interessato sono ormai considerati come dati personali con capacità di identificazione di un soggetto e vanno raccolti con modalità peculiari (come il garante ha già avuto modo di osservare) anche con la firma grafometrica (coordinate, tempo, pressione, salti in volo ecc.) e sono assistiti da specifiche garanzie e forme di controllo maggiore, poiché riguardano trattamento dei dati diversi da quelli sensibili e giudiziari con rischi specifici per i diritti e le libertà fondamentali e per la dignità dell'interessato⁴. Si assiste cioè a un utilizzo della tecnica verso l'uomo, in cui il mondo giuridico tenta di colmare la differenza esistente e l'affanno sempre maggiore per il giurista nella traduzione di principi e valori con modalità di garanzia dell'individuo. Senza tema di smentite potremmo osservare come sempre di più il carattere sperimentale di questa scienza si evidenzia nella indicazione di possibili risultati *de iure condendo* che diventano nello spazio di un *bit*, *de iure condito* e già in via di superamento. ©

NOTE

1. Si tratta di una smartcard, resistente all'usura (a tal fine i dati stampati sono protetti da una sottile pellicola trasparente, che viene applicata su entrambi i lati in fase di produzione) e nella struttura originaria conteneva le generalità del titolare; la foto del titolare; il numero del documento; la tipologia del documento; la data di emissione e di validità dello stesso; le generalità dei figli (se ve ne sono); il codice fiscale; il motivo del soggiorno; L'Istituto poligrafico della Zecca dello Stato ha il compito di produrre e attivare il documento, che è rilasciato dal centro elettronico nazionale della Polizia di Stato, mentre la gestione della sicurezza spetta all'Infrastruttura di Sicurezza Pse;
2. Persona che non è cittadino della Unione ai sensi dell'art. 17 par. 1 del Trattato di soggiorno legalmente sul proprio territorio;
3. Si rinvia sul punto al Commento al Provvedimento del Garante su biometria e grafometria 12/11/2014 a cura di L. FOGLIA e G.GARRISI, Digital Document 2014. ◊

Scopri la nuova

SICUREZZA eGIUSTIZIA

con 18 categorie tematiche :

- Approfondimento
- Balistica (new)
- Compliance
- Copyright
- Criminalità Organizzata
- Cultura e Società
- Data Retention
- Digital Forensics
- Diritto Canonico, Eccl. e Vaticano
- Diritto di Internet
- Diritto Penitenziario
- Giurisprudenza
- Lawful Interception
- Leggi e Norme
- Privacy
- Security
- Servizi Postali
- Technology

