[doc. web n. 1501094]

Riconoscimento vocale e gestione di sistemi informatici - 28 febbraio 2008

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Esaminata la richiesta di verifica preliminare presentata da Michelin italiana S.p.A. ai sensi dell'art. 17 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Visti gli atti d'ufficio;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Giuseppe Fortunato;

PREMESSO

1. Trattamento di dati personali biometrici di dipendenti per finalità di reimpostazione della parola chiave dei sistemi informatici

1.1. Michelin italiana S.p.A. ha presentato una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, relativa al trattamento di dati personali dei propri dipendenti per consentire ai medesimi la gestione e la reimpostazione automatica della parola chiave necessaria ad accedere ai sistemi informativi della società *"per riconoscimento vocale tramite telefono"*.

Tale trattamento, basato su un processo di riconoscimento biometrico dell'identità dell'utente mediante l'elaborazione di impronte vocali, verrebbe effettuato con l'ausilio di un'altra società che memorizzerebbe alcune informazioni personali degli utenti su un proprio server situato nella Repubblica federale tedesca. In esso confluirebbero, alimentando un archivio centralizzato (distinto rispetto a quello di altri clienti della medesima società), i seguenti dati personali di ciascun utente: nome, cognome, user-id dell'utente (per la realizzazione della procedura di enrollment) e indirizzo di posta elettronica (per l'invio di una comunicazione automatica dal sistema relativa al corretto completamento della procedura). Anche i profili vocali degli utenti generati nel corso della c.d. fase di addestramento del sistema (descritta al punto 1.2.) verrebbero memorizzati in forma di file criptato e senza riferimenti diretti all'utente loro associato (*"soltanto tramite una tabella pointer della banca dati si può risalire all'abbinamento di questi file anonimi con gli utenti"*: comunicazione Michelin del 22 febbraio 2007, p. 4).

1.2. Al fine del corretto funzionamento del sistema di riconoscimento vocale, in una prima fase (c.d. fase di addestramento, della durata complessiva di circa cinque minuti) gli utenti dovranno *"parlare"* con il sistema, in modo tale da rendere possibile l'acquisizione di informazioni sufficienti (c.d. formazione del vocabolario dell'utente) per consentire la successiva univoca identificazione degli utenti. A tal fine, questi ultimi dovrebbero pronunciare, per quattro volte, tre coppie di parole scelte casualmente in una lista predefinita contenente più di 4000 vocaboli (c.d. *enrollment*). A giudizio della società richiedente *"il timbro della voce non può essere riprodotto e non è possibile riutilizzare il profilo della voce altrove"* (*cfr.* comunicazione del 22 febbraio 2007, p. 2). Inoltre, la trasmissione dei dati tra Michelin e la società che offre il servizio avverrebbe attraverso una rete di dati protetta (Ssl).

Le informazioni vocali così raccolte, a seguito di opportuno trattamento, verrebbero trasformate nel modello (*template*) destinato a essere confrontato con quello risultante ogni qual volta si renda necessario provvedere all'impostazione e reimpostazione della parola chiave. In tali occasioni il sistema procederebbe a un previo confronto tra il dato biometrico risultante dall'analisi delle parole pronunciate dall'utente e il template al medesimo riferito, memorizzato nella fase di addestramento; accertata l'identità dell'utente, il sistema procederebbe automaticamente a impostare la parola chiave, comunicandola al medesimo.

Il sistema di riconoscimento, isolato e non comunicante con altri, non verrebbe utilizzato per ulteriori finalità, né è prevista la comunicazione dei dati a terzi (cfr. comunicazione del 22 febbraio 2007, p. 4).

2. Dati biometrici e disciplina di protezione dei dati personali: principi di liceità, finalità e pertinenza nel trattamento

2.1. Il caso sottoposto alla verifica preliminare di questa Autorità integra un'ipotesi di trattamento di dati personali. Sia le impronte vocali, sia i dati da esse ricavati e successivamente utilizzati per verifiche e raffronti nelle procedure di autenticazione o di identificazione sono informazioni personali riconducibili ai singoli interessati (art. 4, comma 1, lett. b), del Codice), alle quali trova applicazione la disciplina contenuta nel Codice (*cfr*. Provv. 19 novembre 1999, in

Boll. n. 10, p. 68, doc. *web* n. 42058 e 21 luglio 2005, in Boll. n. 63, doc. *web* n. 1150679; in merito v. pure il documento di lavoro sulla biometria del Gruppo art. 29, direttiva n. 95/46/Ce -WP80-, punto 3.1.).

I dati biometrici, per la loro peculiare natura, richiedono l'adozione di elevate cautele al fine di prevenire possibili pregiudizi ai danni degli interessati, con particolare riguardo a condotte illecite che determinino l'abusiva *"ricostruzione"* dell'impronta vocale, la cui possibilità allo stato viene esclusa, partendo dal template e la sua ulteriore *"utilizzazione"* all'insaputa degli stessi.

2.2. Nella fattispecie in esame, la finalità perseguita dalla società è, in termini generali, lecita: infatti, l'adozione di un sistema di autenticazione informatica (mediante il quale gli incaricati dotati di apposite credenziali possono effettuare specifici trattamenti di dati personali), conforme ai requisiti tecnici indicati dalle regole da 1 a 11 dell'Allegato B) al Codice, costituisce una misura di sicurezza che il titolare, il responsabile (ove designato) e l'incaricato sono tenuti ad utilizzare (art. 34, comma 1, lett. a) del Codice).

In linea di principio, non sussistono ostacoli alla predisposizione di un sistema più elevato di sicurezza per le procedure connesse alla gestione delle credenziali di autenticazione, nel caso di specie ricorrendo alle caratteristiche biometriche dell'incaricato (*cfr*. pure regola 2 dell'allegato B) cit.).

Tenuto conto delle caratteristiche tecniche del sistema, nei termini in cui sono state descritte, alla luce dello stato di evoluzione della tecnologia informatica biometrica e considerate le misure di sicurezza attestate da Michelin anche in riferimento alla società che offre in outosourcing il servizio, può ritenersi ammissibile nel caso di specie la centralizzazione in un database delle informazioni personali (in forma di *template* dell'impronta vocale) trattate nell'ambito del descritto procedimento di riconoscimento biometrico: allo stato, infatti, l'impronta vocale della persona, nelle forme in cui essa è acquisita e codificata nella specifica applicazione sottoposta a verifica preliminare, non rappresenterebbe un dato biometrico suscettibile di essere in concreto utilizzato per finalità diverse da quella perseguita dal titolare del trattamento.

L'impronta vocale dell'utente (generata secondo il processo descritto) sarebbe utilizzabile solo per il sistema in esame, e non per eventuali ulteriori diverse applicazioni basate su ulteriori e distinti sistemi di riconoscimento vocale.

3. Adempimenti

Resta fermo il principio secondo cui la società dovrà richiedere il consenso degli interessati (art. 23 del Codice; cfr. pure, tra i tanti, Provv. 1° febbraio 2007, punto 3.3., doc. *web* n. 1381983; Provv. 26 luglio 2006, punto 3.3. doc. *web* n. 1318582; Provv. 15 giugno 2006, punto 3.2., doc. *web* n. 1306523), predisponendo o mantenendo sistemi alternativi per consentire la reimpostazione della password. Resta parimenti fermo l'obbligo della società di rispettare le disposizioni di legge in tema di:

- designazione quale *"responsabile del trattamento"* della società che opera nell'interesse di Michelin per consentire il funzionamento del descritto sistema di riconoscimento biometrico (art. 29 del Codice);
- notificazione al Garante del trattamento dei dati biometrici, anteriormente al suo inizio (artt. 37, comma 1, lett. a), e 38 del Codice);
- attuazione di ogni misura, anche minima, di sicurezza prescritta dal Codice (art. 31 ss. e Allegato B), anche per ciò che riguarda il rilascio dall'installatore del sistema del prescritto attestato di conformità e la relativa conservazione presso la propria struttura (regola n. 25 del Disciplinare tecnico in materia di misure minime di sicurezza-Allegato *"B"* al Codice).

Michelin italiana S.p.A. dovrà altresì provvedere ad adottare, ai sensi dell'art. 17 del Codice, i seguenti accorgimenti:

a. mettere a disposizione di ciascun utente, unitamente all'informativa che la società deve fornire ai sensi dell'art. 13 del Codice, anche con modalità informatiche, le istruzioni per gli utilizzatori (rimesse peraltro a questa Autorità in allegato alla comunicazione del 7 luglio 2006);

b. porre in essere idonee misure organizzative per prevenire ogni rischio di abusivo utilizzo dei dati personali raccolti nella fase di addestramento (ad esempio, prevenendo la presa di conoscenza da parte di soggetti non autorizzati delle coppie di vocaboli memorizzati dagli utenti);

c. curare la tempestiva cancellazione dei dati personali necessari al funzionamento del descritto sistema, anche presso il responsabile del trattamento, successivamente alla cessazione del rapporto di lavoro o di collaborazione con l'utente.

TUTTO CIÒ PREMESSO IL GARANTE

in sede di verifica preliminare ai sensi degli artt. 17 e 154, comma 1, lett. c), del Codice in materia di trattamento di dati personali correlato all'utilizzo di un sistema di riconoscimento biometrico basato sul rilevamento delle impronte vocali da parte di Michelin italiana S.p.A., volto a consentire l'impostazione delle credenziali di autenticazione, prescrive alla medesima società, quali accorgimenti a garanzia degli interessati, di:

- mettere a disposizione di ciascun utente, anche con modalità informatiche, idonee istruzioni per gli utilizzatori (punto 3);
- porre in essere idonee misure organizzative per prevenire ogni rischio di abusivo utilizzo dei dati personali raccolti nella fase di addestramento (punto 3);
- curare la tempestiva cancellazione dei dati personali necessari al funzionamento del descritto sistema, anche presso il responsabile del trattamento, in caso di cessazione del rapporto di lavoro o di collaborazione con l'utente (punto 3).

Roma, 28 febbraio 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli