VEDI ANCHE Newsletter del 12 dicembre 2016

[doc. web n. 5763201]

Verifica preliminare. Utilizzo di un servizio di riconoscimento biometrico come sistema di autenticazione - 27 ottobre 2016

Registro dei provvedimenti
n. 438 del 27 ottobre 2016

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito "Codice");

VISTO il provvedimento generale del Garante n. 513 del 2014 in tema di biometria e le annesse Linee guida in materia di riconoscimento biometrico e firma grafometrica (in G.U. 2.12.2014, n. 280);

ESAMINATA la richiesta di verifica preliminare presentata da Consorzio per il Sistema Informativo - CSI Piemonte ai sensi dell'articolo 17 del Codice;

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 la prof.ssa Licia Califano;

PREMESSO

1.1. Il Consorzio per il Sistema Informativo - CSI Piemonte (di seguito, il consorzio) ha presentato ai sensi dell'articolo 17 del Codice una richiesta di verifica preliminare (pervenuta in data 1° febbraio 2016, successivamente integrata), in relazione al trattamento di dati personali biometrici - basato su sistemi di riconoscimento vocale e facciale - nell'ambito della partecipazione al progetto PIDaaS (Private IDentity as a Service), co-finanziato dal Programma quadro per l'innovazione e la competitività dell'Unione europea.

In qualità di partecipante al progetto europeo, il consorzio intende effettuare una "prima fase di sperimentazione" coinvolgendo i propri dipendenti che, per accedere al servizio di visualizzazione della busta paga e altri documenti "Cedolino on-line", potranno "utilizzare il servizio di riconoscimento biometrico di PIDaas come sistema di autenticazione […] esclusivamente su base volontaria" (istanza cit., p. 5).

In particolare, secondo quando rappresentato nell'istanza:

a. l'utilizzo del sistema biometrico da parte dei dipendenti coinvolgerà inizialmente "un campione ristretto di 200 utenti selezionati [mentre] in un secondo tempo il test verrà esteso a tutti i dipendenti del CSI-Piemonte" (istanza cit., p. 5);

b. i vantaggi del sistema che si intende adottare consistono nella "maggiore usabilità rispetto all'attuale accesso con username e password"; nella "riduzione dei costi legati al ciclo di vita delle credenziali" nonché nell'incremento della sicurezza del sistema (istanza cit., p. 7);

c. l'accesso al servizio "Cedolino on line" consente ai dipendenti di "visualizzare e scaricare: il cedolino mensile […]; il modello C.U. (Certificazione Unica dei Redditi da Lavoro); la comunicazione periodica relativa alla propria posizione assicurativa per chi aderisce al Fondo Pensione" (istanza cit., p. 5);

d. l'attuale sistema di accesso al servizio basata sull'assegnazione di credenziali aziendali "resterà in ogni caso attiva" (istanza cit., p. 6);

e. al fine di poter accedere al sistema il dipendente dovrà "scaricare l'applicazione PIDaaS sul proprio dispositivo mobile" e procedere alla creazione di un proprio account identificato dall'indirizzo email aziendale (operazione che prevede anche la scelta di un PIN); subito dopo il sistema procede alla registrazione dei dati biometrici (a scelta dell'utente riconoscimento solo vocale,

riconoscimento solo facciale, riconoscimento vocale e facciale che costituisce la scelta preimpostata) (istanza cit., p. 8-9);

f. "a partire dai campioni biometrici acquisiti l'applicazione, applicando i BTPS […], genera le "pseudoidentità" e le invia al server dove avviene l'attivazione dell'account utente identificato dall'email" (istanza cit., p. 10);

g. per accedere al servizio Cedolini l'utente deve altresì associare l'account PIDaaS con il proprio codice fiscale (istanza cit., p. 10);

h. in occasione della procedura di autenticazione "il modulo BTPS presente sul server effettua un confronto uno a uno con i riferimenti biometrici di default che sono associati all'account utente. Se la verifica va a buon fine i nuovi modelli vengono salvati sulla base dati e diventano i riferimenti biometrici per il servizio specifico" (istanza cit., p. 11);

i. in caso di applicazione del sistema di riconoscimento vocale "solo durante la fase di test del sistema i modelli biometrici ricavati dall'acquisizione della sola impronta vocale sul dispositivo mobile vengono salvati anche sul server di PIDaaS e utilizzati per effettuare la verifica per confronto diretto con il riferimento biometrico senza utilizzo di BTPS" (istanza cit., p. 17);

j. quanto alla conservazione dei dati "il database dove sono archiviati i riferimenti biometrici generati nel corso del processo sono ubicati presso il data center della società Eurecat, con sede a Barcellona" (istanza cit., p. 19);

k. "gli utenti possono gestire i propri riferimenti biometrici in ogni momento dal dispositivo mobile […] Per ogni riferimento biometrico viene indicata la data di scadenza che coincide con la conclusione della sperimentazione. L'utente ha sempre la facoltà di rinnovare oppure revocare il riferimento biometrico" (istanza cit., p. 18);

l. "l'utente può stabilire autonomamente la durata della validità dei propri modelli biometrici e, qualora lo ritenga necessario, procedere alla loro immediata cancellazione" (istanza cit., p. 20);

1.2. A seguito di una richiesta di chiarimenti ed integrazioni formulata dall'Autorità, il consorzio ha precisato che:

a. "tutti i riferimenti biometrici acquisiti nel corso della sperimentazione […] saranno cancellati al termine della fase sperimentale" (cfr. nota 14.6.2016, p. 3);

b. "l'utilizzo di entrambe le caratteristiche biometriche è motivato dall'esigenza di testare nel pilota tutte le funzionalità della piattaforma" (cfr. nota cit., p. 3);

c. "le operazioni di trattamento effettuate dalla società spagnola Eurecat sulle pseudoidentità archiviate sul database PIDaaS si limitano all'eventuale ripristino del corretto funzionamento del sistema a fronte di un'anomalia segnalata" (cfr. cit., p. 4);

d. "tutti i partner del progetto provengono da paesi appartenenti all'Unione europea ad eccezione del partner norvegese [Norvegian University of Science and Technology] che è incaricato di realizzare i moduli che implementano la tecnologia BTPS. Le attività di valutazione del BTPS […] prevedono […] l'analisi «offline» dei campioni biometrici degli utenti, previamente codificati in rappresentazione vettoriale. Si precisa che prima di essere resi disponibili per l'analisi offline i dati vengono resi anonimi sostituendo il dato identificativo dell'utente con una stringa casuale" (cfr. nota cit., p. 4);

e. con riferimento ai dati trattati dal sistema congiuntamente ai dati biometrici "il PIN di quattro cifre scelto dall'utente in fase di creazione dell'account non ha funzione identificativa ma viene utilizzato esclusivamente per proteggere l'app di PIDaaS"; l'indirizzo e-mail aziendale "viene utilizzata esclusivamente come identificativo dell'account su PIDaaS e dev'essere indicata dall'utente al momento della creazione dell'account […]. L'utente ha comunque in ogni momento la facoltà di modificare tale identificativo sostituendolo con un indirizzo personale"; il codice fiscale, infine, è utilizzato "per attivare l'associazione tra l'account di PIDaaS […] e il Service Provider, nel caso specifico Cedolini" (cfr. nota 14.6.2016, p. 5);

f. i dati trattati relativi "agli accessi effettuati dai dipendenti del servizio Cedolino on line" saranno conservati dal sistema "per la durata di sei mesi dall'acquisizione"; tale conservazione "è totalmente indipendente dalla sperimentazione del progetto […]. Questa ritenzione, come quella relativa a tutta la navigazione anche verso l'esterno della rete aziendale, [è] nota ai dipendenti perché spiegata nel Disciplinare interno per l'utilizzo degli strumenti aziendali" (cfr. nota cit., p. 7);

g. "i campioni biometrici non vengono conservati sul server ma sono cancellati al termine dell'operazione di generazione della rappresentazione vettoriale la cui durata è dell'ordine di pochi secondi" (cfr. nota cit., p. 8);

h. intende fornire agli interessati una specifica informativa in ordine al trattamento da effettuarsi nell'ambito del progetto PIDaaS, trasmettendo il relativo modulo (cfr. nota cit., allegato 1).

1.3. Con successiva nota il consorzio ha ulteriormente chiarito che:

a. nell'ambito del progetto PIDaaS "ciò che viene archiviato su database per ogni utente è una stringa di hash (Pseudoidentità o PI)" (cfr. nota 19.9.2016, p. 2);

b. "la procedura di registrazione è disponibile nella sezione dell'intranet aziendale del CSI-Piemonte […], alla quale si accede autenticandosi con le credenziali aziendali già in possesso del dipendente" (cfr. nota cit., p. 3);

c. "obiettivo del pilota è confermare in uno scenario e con utenti reali i risultati ottenuti in laboratorio" (cfr. nota cit., p. 3);

d. "l'accesso al servizio cedolini on line tramite riconoscimento biometrico dell'utente sarà attivato come modalità alternativa rispetto all'attuale per cui si richiede la verifica di credenziali aziendali. [Pertanto] ogni volta che l'utente decide di accedere al proprio cedolino potrà scegliere tra due diverse modalità entrambe disponibili sulla home page del servizio" (cfr. nota cit., p. 4).

1.4. Il consorzio ha da ultimo precisato che "previo ottenimento dell'autorizzazione, la sperimentazione del servizio in oggetto avverrà nel periodo 24/10/2016-31/01/2017" (cfr. nota 12.10.2016).

2.1. Il trattamento di dati biometrici, data la loro delicatezza, può essere effettuato previa adozione di particolari cautele; tali dati, infatti, come ha ribadito il Garante, sono "direttamente, univocamente e in modo tendenzialmente stabile nel tempo, collegati all'individuo e denotano la profonda relazione tra corpo, comportamento e identità della persona" (cfr. Provvedimento 12 novembre 2014, n. 513, reperibile in www.garanteprivacy.it, doc. web nn. 3556992 e 3563006).

I titolari che intendono trattare dati biometrici, dovranno, pertanto, sia conformare i relativi trattamenti ai principi generali di liceità, finalità, necessità e proporzionalità, sia adottare le misure e gli accorgimenti tecnici, organizzativi e procedurali eventualmente prescritti dall'Autorità in relazione a talune specifiche tipologie di trattamento all'esito di una verifica preliminare (artt. 3, 11 e 17 del Codice).

Sotto il profilo sostanziale, il trattamento che il consorzio intende effettuare, in ragione delle specificità del sistema utilizzato e della particolare tipologia di dati biometrici trattati, non rientra nei casi di esonero dalla verifica preliminare previsti dal citato provvedimento del Garante.

Il presente provvedimento è riferito esclusivamente ai trattamenti effettuati per le menzionate finalità di ricerca scientifica e limitatamente al periodo di sperimentazione dichiarato, che, entro tali limiti, risultano –come si vedrà- nel complesso leciti.

Il provvedimento non riguarda, invece, eventuali future applicazioni "a regime" del sistema di autenticazione progettato, che - se del caso - saranno valutate dall'Autorità, in termini di liceità e di proporzionalità, alla luce delle particolarità dei casi concreti che i rispettivi titolari del trattamento sottoporranno eventualmente a verifica preliminare innanzi al Garante (art. 17 del Codice).

2.2. Il trattamento in esame è finalizzato a testare in un contesto "reale" e per un periodo di tempo limitato (pochi mesi) un innovativo servizio di autenticazione informatica basato sul riconoscimento dell'immagine del volto e dell'impronta vocale, verificandone l'accuratezza, la facilità d'uso e la sicurezza (compresi i profili di protezione dei dati personali). Il consorzio, in tale prospettiva, ha elaborato un progetto pilota che prevede l'applicazione del sistema di autenticazione basato su tecnologie biometriche al sistema di accesso al servizio Cedolini on-line da parte dei dipendenti, in alternativa al sistema in uso basato sull'utilizzo di credenziali di autenticazione (user-id e password).

Le finalità del prospettato trattamento sono, quindi, di tipo scientifico, diverse da quelle perseguite nell'ambito delle attività di gestione dei rapporti di lavoro con i dipendenti del consorzio.

Il consorzio, che ha personalità giuridica di diritto pubblico (cfr. l. reg. Piemonte 4.9.1975, n. 48 e 15.3.1978, n. 13 e succ. mod. e att.), può effettuare trattamenti di dati personali (diversi dai dati sensibili e giudiziari) per lo svolgimento delle proprie funzioni istituzionali (artt. 18 e 19 del Codice). Tra le attività istituzionali svolte risulta espressamente indicata la promozione e realizzazione di "forme di collaborazione continuativa tra Enti pubblici ed Atenei nei campi […] della ricerca e sviluppo di nuove tecnologie dell'informazione, della comunicazione e della conoscenza" nonché lo svolgimento di ulteriori attività consistenti nella progettazione, sviluppo e commercializzazione di "prodotti, servizi e sistemi informativi" (cfr. "Statuto del C.S.I. Piemonte", artt. 4, 5 e 6).

Da questo punto di vista, pertanto, il trattamento oggetto di verifica preliminare risulta in termini generali lecito.

Il trattamento prospettato, che rientra astrattamente tra le citate attività istituzionali proprie del consorzio, può essere effettuato conformemente ai principi posti dal Codice, alle pertinenti disposizioni specifiche previste in caso di trattamento di dati personali effettuato per scopi scientifici (cfr. artt. 97-100, 104 e 105 del Codice) e al Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici (Provvedimento del Garante n. 2 del 16 giugno 2004, All. 4 del Codice, in G. U. 14.8.2004, n. 190). In particolare, in applicazione del principio di finalità, i trattamenti di dati effettuati per scopi scientifici "non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né per trattamenti di dati per scopi di altra natura" (cfr. art. 105, comma 1, cit.).

2.3. Le operazioni di trattamento prospettate risultano altresì, nel complesso, coerenti con i principi di necessità, pertinenza e non eccedenza (cfr. artt. 3 e 11, comma 1, lett. d) del Codice) in relazione alle finalità sperimentali e temporanee del progetto, alla luce delle seguenti caratteristiche: volontarietà della partecipazione, facoltà di scelta tra i due modelli di autenticazione disponibili garantita in occasione di ciascun singolo accesso al servizio Cedolini, possibilità per l'interessato di chiedere in ogni momento la cancellazione dei modelli biometrici a sé riferiti, cancellazione di tutti i modelli biometrici al termine del progetto.

2.4. Da ultimo e sotto diverso profilo, si richiama l'attenzione su quanto dichiarato dalla società a proposito del trattamento di dati personali tratti dall'utilizzo di strumenti forniti in dotazione ai dipendenti ed effettuati dal consorzio per finalità di gestione del rapporto di lavoro (dati relativi "agli accessi effettuati dai dipendenti del servizio Cedolino on line" che saranno conservati dal sistema "per la durata di sei mesi dall'acquisizione"; tale conservazione, "totalmente indipendente dalla sperimentazione del progetto", ha altresì ad oggetto "tutta la navigazione anche verso l'esterno della rete aziendale": cfr. par. 1.2., lett. f.).

Non essendo, allo stato, presenti in atti elementi sufficienti a valutare la conformità ai principi e alle regole previsti dal Codice di tali trattamenti, anche in relazione al contenuto del Disciplinare interno per l'utilizzo degli strumenti aziendali, solo citato dalla società, l'Autorità si riserva di acquisire presso il titolare ulteriore documentazione rispetto a quella già pervenuta.

3. Ciò premesso, considerate le peculiarità del progetto che il consorzio ha intenzione di realizzare - in particolare, l'avvalimento della collaborazione dei propri dipendenti in occasione dell'utilizzo del servizio di accesso a documentazione riferita al rapporto di lavoro, il trattamento congiunto di due particolari tipologie di dati biometrici e la prevista partecipazione al progetto di un partner europeo - si ritiene tuttavia necessario prescrivere con il presente provvedimento alcune misure ed accorgimenti a tutela dei diritti degli interessati, anche alla luce delle pertinenti disposizioni contenute nel menzionato Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici, nei termini di seguito esposti.

3.1. Il consorzio, in applicazione del principio di finalità, dovrà adottare misure volte a garantire che il trattamento oggetto di sperimentazione sia in concreto effettuato con modalità del tutto autonome dall'operatività dei sistemi utilizzati per finalità di gestione del rapporto di lavoro. In tale prospettiva dovranno essere implementate politiche di segregazione dei dati e dei sistemi per far sì che la sperimentazione non possa coinvolgere sistemi e applicativi aziendali usualmente utilizzati dal consorzio. A titolo esemplificativo, gli utenti che decideranno di aderire alla sperimentazione non potranno accedere all'applicativo Cedolino on-line in uso, bensì ad un'apposita istallazione di test creata appositamente per tale progetto e contenente solo i cedolini degli utenti stessi.

Inoltre dovranno essere fornite credenziali ad hoc ed un indirizzo di posta elettronica temporaneo da utilizzare per accedere alla sezione della intranet da cui si avvia la fase di enrollment e per effettuare il login all'applicazione PIDaaS.

La cancellazione dei dati biometrici al termine della sperimentazione (o a seguito di specifica richiesta del partecipante) dovrà essere irreversibile.

3.2. Posto che, secondo quanto riferito, il progetto prevede la comunicazione di alcuni dati personali riferiti ai partecipanti al partner spagnolo del progetto (EURECAT-Technology Centre of Catalonia, mentre secondo quanto dichiarato i dati condivisi con altri due partner sono previamente anonimizzati), il consorzio con propria determinazione dovrà individuare i termini e le condizioni delle operazioni di comunicazione e del successivo trattamento dei dati conferiti, compreso il profilo della sicurezza (cfr. art. 100, comma 1, del Codice). In particolare, fermo restando l'obbligo di comunicare al Garante il verificarsi di violazioni dei dati biometrici (data breach) o incidenti informatici previsto dal paragrafo 3 del Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014, il consorzio dovrà predisporre una procedura per la gestione congiunta degli eventuali incidenti di sicurezza che dovessero occorrere ai sistemi informatici che ospitano i servizi PIDaaS e al database dove risiedono i modelli biometrici, individuando altresì le ipotesi nelle quali prevedere la comunicazione agli interessati della violazione dei dati biometrici che li riguardano. Le operazioni di irreversibile cancellazione dei dati biometrici da effettuarsi al termine del progetto dovranno altresì essere dettagliatamente documentate dal partner e la relativa documentazione sarà acquisita dal consorzio. Dovrà essere data notizia agli interessati dell'avvenuta effettuazione delle operazioni di cancellazione dei dati.

4. Resta fermo che il consorzio - come del resto, per alcuni aspetti, già rilevato nell'istanza - è tenuto in base alla normativa vigente a:

a. effettuare la notificazione al Garante ai sensi dell'articolo 37, comma 1, lett. a), del Codice;

b. fornire agli interessati un'informativa comprensiva di tutti gli elementi contenuti nell'articolo 13 del Codice, anche in conformità al principio di correttezza in base al quale il titolare è tenuto a rendere chiaramente riconoscibili agli interessati i trattamenti che intende effettuare (art. 11, comma 1, lett. a), del Codice);

c. predisporre misure al fine di garantire agli interessati l'esercizio dei diritti previsti dagli articoli 7 e seguenti del Codice (anche alla luce di quanto stabilito dall'art. 100, comma 2, del Codice).

TUTTO CIÒ PREMESSO IL GARANTE

preso atto della richiesta di verifica preliminare presentata dal Consorzio per il Sistema Informativo - CSI Piemonte, ai sensi dell'articolo 17 del Codice prescrive che il consorzio, quali misure necessarie, dovrà:

a. avvalersi, nell'ambito del progetto, di sistemi ed applicativi informatici distinti da quelli utilizzati per finalità di gestione del rapporto di lavoro (punto 3.1.);

b. fornire agli utenti coinvolti nella sperimentazione credenziali ad hoc ed un indirizzo di posta elettronica temporaneo da utilizzare per accedere alla sezione della intranet da cui si avvia la fase di enrollment e per effettuare il login all'app PIDaaS (punto 3.1.);

c. individuare, con propria determinazione, i termini e le condizioni delle operazioni di comunicazione e del successivo trattamento dei dati conferiti al partner del progetto, compreso il profilo della sicurezza, individuando in particolare (punto 3.2.):

- una procedura per la gestione congiunta degli eventuali incidenti di sicurezza che dovessero riguardare i sistemi informatici che ospitano i servizi PIDaaS e il database dove risiedono i modelli biometrici;

- i casi in cui gli interessati dovranno essere informati di eventuali violazioni dei dati biometrici che li riguardano;

- le modalità di documentazione dell'avvenuta irreversibile cancellazione dei dati al termine della sperimentazione; tale documentazione sarà acquisita dal consorzio e dell'avvenuta cancellazione dovrà essere data notizia agli interessati;

d. adottare, al termine della sperimentazione o a seguito di specifica richiesta del partecipante, modalità

irreversibili di cancellazione dei dati biometrici (punto 3.1.).

Ai sensi degli articoli 152 del Codice e 10 del decreto legislativo n. 150 del 2011, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 27 ottobre 2016

IL PRESIDENTE
Soro

IL RELATORE
Califano

IL SEGRETARIO GENERALE
Busia