[doc. web n. 2304808]

Trattamento di dati biometrici. Verifica preliminare richiesta da Unicredit S.p.A. - 31 gennaio 2013

Registro dei provvedimenti
n. 37 del 31 gennaio 2013

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

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

VISTA la richiesta di verifica preliminare del 21 settembre 2012, presentata da Unicredit S.p.A. ai sensi dell'art. 17 del Codice e regolarizzata con comunicazione del 29 novembre 2012;

ESAMINATA la documentazione in atti;

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

RELATORE il dott. Antonello Soro;

PREMESSO

1. La richiesta formulata dalla società.

Con nota del 21 settembre 2012, Unicredit S.p.A., in vista di un "accrescimento della qualità di erogazione dei propri servizi", ha dichiarato di voler rendere disponibile a vantaggio (anche) della clientela un servizio di sottoscrizione dei documenti con firma digitale basato su una procedura di autenticazione biometrica effettuata tramite signpad (c.d. "tablet"), volta a conferire, tra l'altro, maggiore sicurezza nello svolgimento delle operazioni allo sportello. Il sistema, secondo quanto riferito, raccoglierebbe le caratteristiche biometriche di natura comportamentale del cliente, rilevando e, in pari tempo, analizzando alcuni parametri (ritmo; velocità; pressione; accelerazione; movimento) relativi alla sua firma autografa –apposta per il tramite di un dispositivo hardware "dedicato" e collegato via USB (Universal Serial Bus) al terminale dell'operatore di filiale a ciò preposto– al fine di confrontarli con quelli precedentemente memorizzati in fase di adesione al "servizio". L'eventuale comparazione positiva, che determinerebbe l'autenticazione dell'utente, consentirebbe l'avvio della procedura di sottoscrizione con firma digitale del documento visionato dal cliente.

L'adozione di tale sistema, a detta della società, permetterebbe, tra l'altro, "di sviluppare una serie di numerosi vantaggi, anche a beneficio della clientela", potendo garantire una "maggiore sicurezza contro i tentativi di frode" attraverso la riduzione dei "rischi di furto di identità e [di] contraffazione della firma".

2. Il funzionamento del sistema e le modalità del trattamento dei dati biometrici ad esso connesso.

2.1. Secondo quanto sinteticamente prospettato, il sistema opererebbe nei termini di seguito indicati.

Il cliente che intendesse aderire al servizio, una volta rilasciato il proprio consenso informato al trattamento, verrebbe invitato, durante la fase di enrollment, ad apporre 6 firme sul "tablet" ai fini del "riconoscimento" biometrico; le informazioni raccolte (c.d. specimen), acquisite dal sistema in misura pertinente e non eccedente rispetto alle finalità del servizio e in forma "acritica" –con modalità tali, cioè, da non consentire, nemmeno accidentalmente, di poter risalire ad eventuali patologie dell'utente– verrebbero inviate al "biometric server" ai fini della loro immediata conversione, attraverso un algoritmo di hash, in una sequenza di caratteri ("stringa") immodificabile e non reversibile nel dato biometrico "originario".

Successivamente alla fase di enrollment, in occasione della sottoscrizione dei documenti con firma digitale, il cliente sarebbe invitato, di volta in volta, ad apporre la propria firma sul tablet per la relativa autenticazione: i dati biometrici così ricavati verrebbero confrontati con quelli precedentemente memorizzati dal sistema, il quale consentirebbe l'avvio delle procedure di apposizione della firma digitale solo in caso di "matching" positivo. A seguito dell'autenticazione biometrica, infatti, le chiavi crittografiche, detenute da In.Te.S.A. S.p.A. (autorità certificata presso l'Agenzia per l'Italia Digitale, già DigitPA) all'interno di dispositivi sicuri denominati Hardware Security Module (HSM), verrebbero rese disponibili ai fini della sottoscrizione con firma digitale dei documenti visionati dall'interessato.

Il sistema, "grazie ad una funzione di auto apprendimento (continuous enrollment)", sarebbe in grado di aggiornare costantemente il "profilo" dell'utente originariamente registrato, sì da garantire comunque la possibilità di avvalersi del servizio anche in caso di eventuali modifiche, nel corso del tempo, dello "stile di firma"; inoltre, sarebbe configurato "con una soglia minima di accettazione della verifica della firma

(cosiddetto score) pari all'80% di rispondenza rispetto al template creato originariamente", in modo tale da garantire, "in punto di verifica delle firme (trade-off falsi positivi vs falsi negativi) […] un elevato livello di credibilità ed affidabilità", peraltro ulteriormente incrementabile a seguito di periodici monitoraggi e verifiche che la società ha dichiarato di voler effettuare.

I dati biometrici acquisiti, immediatamente criptati e indicizzati con codici univoci associati ai clienti, sarebbero memorizzati in server variamente ubicati sul territorio nazionale presso le strutture di Unicredit S.p.A. e Unicredit Business Integrated Solutions S.c.p.a. (società deputata, per conto della prima, alla gestione e alla fornitura dei sistemi informativi e delle relative infrastrutture tecniche), designata responsabile del trattamento ai sensi degli artt. 4, comma 1, lett. g) e 29 del Codice. Inoltre, gli stessi dati, fatta salve l'eventuale revoca del consenso da parte degli interessati e le esigenze di ulteriore conservazione dettate da eventuali contestazioni, verrebbero conservati per la durata del servizio.

La società, al fine di garantire elevati standard di sicurezza, ha dichiarato di aver adottato, unitamente alle misure minime di cui all'allegato "B" al Codice, "tutte le ulteriori misure di sicurezza, in linea con l'attuale conoscenza tecnica e tecnologica, volte ad ottenere l'irreversibilità dei dati grafometrici, l'immodificabilità degli stessi, nonché ad escluderne il rischio di corruzione e sottrazione". In particolare, ha dichiarato che i dati biometrici degli interessati, criptati mediante chiavi di cifratura (a loro volta cifrate attraverso un certificato digitale precedentemente prodotto), risultano immutabili e irreversibili; inoltre, anche i flussi comunicativi tra le varie "componenti dell'infrastruttura avvengono in modalità autenticata e cifrata", mentre "gli accessi [risultano] registrati nell'audit log del sistema e resi disponibili" per eventuali controlli.

Il processo di autenticazione, così come descritto, sarebbe "autonomo e distinto rispetto alle procedure di firma delle disposizioni bancarie e/o di sottoscrizione di contratti" con la banca. L'apposizione della firma sul tablet, infatti, costituirebbe "unicamente l'elemento da cui scaturisce il processo di autenticazione, risultando così prodromico al processo di firma". A conferma di ciò, la società ha dichiarato che la "certification authority […] non è in alcun modo coinvolta nel processo di trattamento del dato grafometrico", intervenendo quest'ultima "esclusivamente nel processo di firma dei documenti" e in vista "della creazione e gestione del certificato qualificato e delle chiavi per la firma".

2.2. L'informativa che la società intende fornire agli interessati antecedentemente alla fase di enrollment "sarà ulteriore e distinta rispetto a quella generale consegnata a tutta la clientela in occasione dell'instaurazione del rapporto con Unicredit" e indicherà espressamente il carattere "facoltativo" del trattamento. Quest'ultimo, inoltre, "sarà subordinato all'espressa manifestazione di un consenso da parte degli interessati […] revoca[bile] in qualsiasi momento". La società, poi, ha dichiarato che provvederà a designare gli incaricati del trattamento "impartendo loro idonee istruzioni sul funzionamento degli strumenti e sulle modalità di apposizione della firma digitale", precisando altresì di aver già provveduto a modificare la notificazione del trattamento in data 7 giugno 2012 (circostanza, questa, verificata dall'Autorità).

2.3. La scelta di dotarsi del sistema in esame, a detta della società istante, risponderebbe alla necessità, tra l'altro, di identificare rigorosamente la clientela in occasione dello svolgimento delle operazioni bancarie, in conformità agli obblighi a tal fine previsti dalla normativa in materia di antiriciclaggio (d.lgs. n. 231/2007). Inoltre, l'utilizzo del dato biometrico –ritenuto idoneo, come detto, a prevenire e contrastare fenomeni fraudolenti legati, soprattutto, al furto di identità– garantirebbe il firmatario dall'ulteriore rischio di smarrimento degli altri strumenti (smart card, token usb, ecc.) necessari ai fini dell'attivazione delle procedure di sottoscrizione dei documenti con firma digitale.

3. Le osservazioni dell'Autorità.

3.1. La verifica preliminare presentata all'Autorità ha ad oggetto il trattamento di dati biometrici a fini di autenticazione connesso all'utilizzo di un sistema idoneo ad analizzare e confrontare alcuni parametri ricavati dall'apposizione su un dispositivo a ciò preposto, da parte degli interessati, della loro firma autografa in occasione delle procedure di sottoscrizione con firma digitale dei documenti. Il presente provvedimento, che tiene conto del tenore dell'istanza formulata e delle dichiarazioni rese dalla società istante (anche ai sensi dell'art. 168 del Codice) in ordine all'alterità tra la procedura di sottoscrizione digitale e quella di autenticazione, si sofferma sui soli profili relativi al trattamento dei dati personali biometrici connesso a quest'ultima.

Merita preliminarmente evidenziare, al riguardo, che il Gruppo per la tutela dei dati personali ex art. 29 della direttiva 95/46/Ce ritiene che l'utilizzo di sistemi basati sull'impiego di dispositivi in grado di rilevare le caratteristiche "dinamiche" della firma determini, effettivamente, un trattamento di dati biometrici di natura comportamentale, come tale riconducibile nell'ambito di applicazione della disciplina di tutela dei dati personali (cfr. documento di lavoro sulla biometria del 1° agosto 2003, Wp 80; cfr. altresì Parere 3/2012 sugli sviluppi nelle tecnologie biometriche del 27 aprile 2012, WP 193). Ciò premesso, occorre valutare, in tale prospettiva, se il sistema sottoposto al vaglio dell'Autorità possa reputarsi conforme, limitatamente ai profili concernenti il trattamento di dati biometrici dei clienti nella fase di autenticazione, alla disciplina del Codice, con particolare riferimento all'osservanza dei principi di necessità, liceità, finalità e proporzionalità (artt. 3 e 11, comma 1, lett. a), b) e d), del d.lgs. n. 196/2003); ciò, anche nel caso in cui il dato biometrico venga raccolto, come nel caso in esame, ai soli fini del completamento della fase di enrollment e venga successivamente utilizzato (sotto forma di codice numerico) per le operazioni di raffronto nelle procedure di autenticazione (in argomento, v. anche Provv. 23 gennaio 2008, doc. web n. 1487903; Provv. 26 maggio 2011, doc. web n. 1832558; Provv. 4 ottobre 2012, doc. web n. 2059743).

3.2. In proposito, occorre rilevare che il trattamento dei dati biometrici che la società istante intende effettuare, in base alla documentazione prodotta e alle dichiarazioni rese, risulta lecito. Vale infatti sottolineare, sul piano generale, che l'identificazione certa e rigorosa della clientela, già richiesta alle banche in un'ottica di sana e prudente gestione del rischio (cfr. Comitato di Basilea per la vigilanza bancaria), rappresenta, sovente, anche un obbligo posto in capo a tutti gli istituti di credito da specifiche normative di settore (cfr., ad esempio, il d.lgs. n. 231/2007, su cui v. anche Parere Garante del 25 luglio 2007, doc web n. 1431012; più in generale, sugli obblighi di identificazione della clientela, cfr. Provv. 27 ottobre 2005, doc. web n. 1189435 e Provv. 25 ottobre 2007, recanti le "Linee guida per i trattamenti dati relativi al rapporto banca-clientela", doc. web n. 1457247) la cui violazione, peraltro, può costituire fonte di eventuale responsabilità civile (cfr. Cass. 16 dicembre 2009, n. 3350), valutabile anche alla stregua dell'art. 1176, 2° co., c.c. (con possibile rilevanza, dunque, anche della colpa lieve: in tal senso, Trib. Ariano Irpino 2 ottobre 2008; Cass. 30 gennaio 2006, n. 1865). A ciò, si aggiunga che l'autenticazione biometrica dei clienti in vista della sottoscrizione digitale dei documenti potrebbe, da un lato, contribuire a contrastare efficacemente eventuali tentativi di frode e, dall'altro, snellire e velocizzare (anche a vantaggio della stessa clientela) le operazioni di riconoscimento allo sportello. Considerato,

poi, che il trattamento dei dati biometrici dei firmatari, nella misura in cui possa ritenersi effettivamente compatibile con l'attuale quadro normativo applicabile ai servizi di sottoscrizione con firma digitale (in tal senso, peraltro, una prima apertura all'utilizzabilità di tecniche biometriche, sia pure nell'ambito del più ampio contesto relativo ai servizi di "firma elettronica", pare ravvisabile già nella "Guida alla Firma Digitale" predisposta dall'allora CNIPA, versione 1.3 dell'aprile 2009, p. 11; in prospettiva, v. lo "Schema di d.P.C.M. ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71, del d. l.gvo 7 marzo 2005, n. 82", disponibile sul sito www.digitpa.gov.it), avverrà sulla base del libero consenso degli interessati e per il perseguimento di legittime finalità rese preventivamente note a questi ultimi, deve ritenersi che, alla luce di quanto sopra richiamato, risultino integrati, rispetto alla fattispecie in esame, i requisiti di cui agli artt. 11, comma 1, lett. a) e b), 13 e 23 del Codice.

Per quanto attiene, poi, all'osservanza dei princìpi di necessità e proporzionalità (artt. 3 e 11, comma 1, lett. d), del Codice), vale sottolineare che il sistema descritto, alla luce delle dichiarazioni rese, risulta preordinato all'acquisizione delle sole informazioni pertinenti rispetto alla finalità di autenticazione degli interessati. Inoltre, il servizio appare configurato, sulla base degli elementi forniti, per raccogliere un numero circoscritto di informazioni (in tal senso, cfr. il modello di informativa prodotto dalla società), non risultando peraltro il sistema, nelle prospettate modalità di configurazione –tali, secondo la società, da non consentire, in nessun caso, l'acquisizione di informazioni relative allo stato di salute degli interessati– predisposto per l'acquisizione di dati ultronei rispetto a quelli necessari ai fini dell'autenticazione.

Sotto il profilo della sicurezza dei dati trattati, si può ritenere che l'immediata cifratura delle informazioni biometriche degli interessati (attraverso una chiave a sua volta cifrata), l'impiego di canali di trasmissione dei dati anch'essi cifrati e l'utilizzo di procedure di autenticazione e di registrazione degli accessi costituiscano misure idonee ai sensi degli artt. 31 e ss. del Codice. Inoltre, anche il fatto che i dati biometrici non risiederanno, neanche per periodi limitati, sui tablet (cfr. Progetto SignPad del 25 giugno 2012) e che i template, non riversibili nell'originario dato biometrico, verranno conservati in database appositamente "dedicati" –misure tali, unitamente a quelle già menzionate, da far ritenere come remoto il rischio di eventuali operazioni indebite sui dati biometrici degli interessati– induce a considerare il prospettato trattamento, sul piano della sicurezza, come conforme alla disciplina del Codice.

Analogamente, anche in ragione di quanto previsto dall'art. 11, comma 1, lett. c) del Codice, va valutata in chiave positiva la scelta di adottare meccanismi di auto-apprendimento, in grado di garantire, nel tempo, la "qualità" dei dati biometrici trattati.

Infine, preso atto che il modello di informativa prodotto in atti dalla banca non presenta profili problematici, si ritiene conforme a legge il fatto che la società, fatta salva l'eventuale applicabilità di specifiche normative, conservi i dati biometrici degli interessati per il periodo di tempo strettamente necessario al perseguimento degli scopi per i quali gli stessi verranno raccolti e successivamente trattati (art. 11, comma 1, lett. e) del Codice), restando comunque impregiudicata la loro ulteriore conservazione in caso di eventuali contestazioni, anche in sede anche giudiziaria. In caso di cessazione del trattamento, ovviamente, i dati dovranno essere cancellati immediatamente, ovvero nei tempi tecnici necessari consentiti dal sistema.

TUTTO CIÒ PREMESSO IL GARANTE

ai sensi dell'art. 17 del Codice, a conclusione della verifica preliminare richiesta da Unicredit S.p.A. relativamente all'utilizzo, nell'ambito del servizio preordinato alla sottoscrizione di documenti con firma digitale, di un sistema di rilevazione delle caratteristiche biometriche della firma autografa apposta dagli interessati su dispositivi a ciò dedicati, ammette il trattamento dei dati biometrici, a condizione che esso avvenga per le sole finalità dichiarate, con le modalità indicate in narrativa e nel doveroso rispetto di quanto dichiarato dall'istante ai sensi dell'art. 168 del Codice.

Ai sensi degli artt. 152 del Codice e 10 del d.lg. n. 150/2011, 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, 31 gennaio 2013

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia