Sistema per la sottoscrizione in forma elettronica di atti, contratti e altri documenti relativi a prodotti e servizi offerti da una banca - Verifica preliminare richiesta da Fineco Bank S.p.A. - 12 settembre 2013

Registro dei provvedimenti
n. 396 del 12 settembre 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.lgs. 30 giugno 2003, n. 196, recante il "Codice in materia di protezione dei dati personali" (di seguito "Codice");

VISTO il d.lgs. 7 marzo 2005, n. 82, recante il "Codice dell'amministrazione digitale";

VISTO il d.P.C.M. 22 febbraio 2013, recante le "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, 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";

VISTO il d.lgs. 1° settembre 1993, n. 385, recante il "Testo unico delle leggi in materia bancaria e creditizia";

VISTO il d.lgs. 24 febbraio 1998, n. 58, recante il "Testo unico delle disposizioni in materia di intermediazione finanziaria, ai sensi degli articoli 8 e 21 della legge 6 febbraio 1996, n. 52";

VISTA la richiesta di verifica preliminare datata 29 aprile 2013 e presentata da Fineco Bank S.p.A. ai sensi dell'art. 17 del Codice, nonché l'ulteriore comunicazione della società del 12 luglio 2013;

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.

1.1. Fineco Bank S.p.A. –società operante "esclusivamente on line e tramite promotori finanziari dislocati su tutto il territorio nazionale"– ha manifestato l'intenzione, nella prospettiva (tra l'altro) di accrescere la qualità dei propri servizi, di volersi dotare di un sistema in grado di consentire la sottoscrizione in forma elettronica di atti, contratti e altri documenti relativi a prodotti e servizi offerti dalla banca attraverso "[…]l'utilizzo combinato di firme elettroniche e […]la raccolta di dati biometrici comportamentali" desunti dalla firma apposta dai clienti su appositi "tablet" in dotazione ai medesimi promotori. Il servizio di "firma grafometrica" (nell'accezione utilizzata dalla banca), che consentirebbe di rilevare le caratteristiche "dinamiche" (ritmo; velocità; pressione; accelerazione; movimento) e il tratto grafico della firma apposta dai clienti in occasione della sottoscrizione dei predetti documenti, avrebbe come obiettivo "principale" la semplificazione e l'efficientamento dei processi di interazione tra la società e i suoi clienti, garantendo in pari tempo a costoro maggiori standard di sicurezza nelle operazioni di sottoscrizione; ciò, in quanto il servizio offerto si configurerebbe come "un particolare tipo di firma elettronica" avanzata in grado di assicurare, in accordo con le previsioni di legge, l'identificabilità dell'autore, nonché l'integrità e l'immodificabilità del documento sottoscritto (v. anche il successivo punto 1.5).

1.2. Il processo che Fineco ha intenzione di adottare si basa su una soluzione di c.d. firma grafometrica sviluppata da Namirial S.p.A. (organismo di certificazione accreditato presso l'Agenzia per l'Italia Digitale) che ha ricevuto la certificazione ISO 27001 relativa al proprio sistema di gestione della sicurezza. Tale processo di firma richiede il trattamento di dati biometrici degli interessati sottoscrittori e consta, in estrema sintesi, delle seguenti fasi:

– i promotori finanziari collaboratori della Banca illustrano al cliente le modalità di fruizione del servizio di "firma grafometrica";

– il promotore rilascia la prevista informativa ex art. 13 del Codice e acquisisce il relativo consenso in caso di adesione al servizio;

– il promotore sottopone al cliente (previamente identificato) il documento in formato elettronico;

– il cliente appone la "firma grafometrica" su un dispositivo hardware in grado di acquisire i dati biometrici contestualmente all'atto di apposizione della firma; tali dati subiscono un processo di cifratura intermedio basato su una chiave simmetrica (che esclude la possibilità di visualizzarli "in chiaro" nella loro interezza) e un'ulteriore cifratura tramite la chiave pubblica relativa a un certificato digitale denominato "certificato di protezione Fineco" anch'essa contenuta nel dispositivo di firma digitale in dotazione ai promotori;

– i dati biometrici così cifrati e il tratto grafico della firma sono inseriti in appositi campi del documento registrato in formato pdf;

– sono generate una serie di stringhe hash per la successiva verifica dell'integrità della firma e dei documenti acquisiti in formato elettronico, anch'esse cifrate con la "chiave pubblica" associata al certificato rilasciato da Namirial S.p.A.;

– il documento informatico sottoscritto viene così inviato tramite canali sicuri al "Sistema documentale di Fineco" e all'"Archivio di conservazione a norma" di In.TE.SA. S.p.A. (società incaricata della gestione documentale in conformità ai requisiti stabiliti dal d.lgs. n. 82/2005) per la relativa conservazione;

– il cliente riceve una copia cartacea del documento sottoscritto con "firma grafometrica" o, in alternativa, il duplicato informatico via posta elettronica.
I dati biometrici, cifrati e "sigillati elettronicamente all'interno del documento informatico cui si riferiscono", verrebbero raccolti dal sistema "in modo assolutamente «acritico»", con modalità tali –cioè– da escludere qualsivoglia possibilità di risalire a eventuali informazioni inerenti lo stato di salute dei firmatari.

Inoltre, tali dati non avrebbero "residenza", nemmeno temporaneamente, all'interno dei "tablet" e, una volta incorporati nel documento, verrebbero "cancellati e sovrascritti d[a]lla memoria (ram) del computer", non risultando conseguentemente visualizzabili né dai promotori finanziari, né da In.TE.SA S.p.A. (che, peraltro, avrebbe solo in carico la mera gestione dei documenti in formato elettronico per conto della banca), né, tantomeno, da Fineco Bank S.p.A. e da Namirial S.p.A.

La banca, infatti, non potrebbe avere accesso "in chiaro " ai "dati grafometrici" incorporati nei documenti elettronici (di cui Namirial S.p.A., peraltro, nemmeno avrebbe la disponibilità) se non attraverso la reciproca collaborazione tra le due società, posto che la chiave privata –necessaria alla loro decifrazione– sarebbe detenuta dal solo organismo certificatore, mentre la custodia delle relative "credenziali di sblocco" sarebbe affidata unicamente alla banca.

In ogni caso, la decifrazione dei dati biometrici e il relativo accesso "in chiaro" sarebbero consentiti "esclusivamente nei casi previsti dalla legge, su richiesta delle Autorità competenti" (tipicamente riconducibili a ipotesi di contenzioso legate al disconoscimento della firma); in tale evenienza, Namirial S.p.A. metterebbe a disposizione del perito calligrafico nominato dall'autorità giudiziaria un apposito strumento (denominato "FirmaCerta Forense") che consentirà di gestire la procedura di decriptazione secondo elevati standard di sicurezza, garantendo che le operazioni di "cifratura e decifratura [si svolgano] contestual[ment]e […] all'apertura e alla chiusura della perizia".

I dati acquisiti nel corso dell'accertamento calligrafico sarebbero cifrati attraverso la "chiave pubblica" del certificato di autenticazione del perito stesso, unico "in grado di aprire la perizia utilizzando il proprio dispositivo di firma".

A detta della banca, il sistema risulterebbe preordinato ad acquisire "un numero circoscritto di informazioni, pertinenti rispetto alle finalità […] indicate, non [essendo] prev[ista] l'acquisizione di dati ultronei o relativi allo stato di salute" degli interessati. Inoltre, il trattamento dei dati biometrici sarebbe "limitato, per tipologia e ampiezza, allo stretto indispensabile per consentire alla banca di aderire ai requisiti normativi previsti dal CAD", di talché "nessun altro trattamento o utilizzo sar[ebbe] possibile".

1.3. Il servizio, così come descritto, verrebbe attivato su base esclusivamente volontaria (con indicazione del carattere facoltativo del conferimento dei dati anche nell'informativa da rendere agli interessati), previa acquisizione del libero consenso di questi ultimi. Ove il cliente non intendesse fornire il proprio consenso al trattamento, ovvero lo abbia successivamente revocato, i documenti resteranno sottoscrivibili secondo "il processo di firma «tradizionale» su supporto cartaceo".

La banca ha poi dichiarato che provvederà a designare In.TE.SA. S.p.A. quale responsabile del trattamento ai sensi dell'art. 29 del Codice, indicando analiticamente i compiti affidatigli e vigilando sulla puntuale osservanza delle istruzioni impartite; per contro, i promotori finanziari, preposti dalla banca alle operazioni di rilevazione dei dati biometrici degli interessati, verrebbero designati quali incaricati del trattamento ex art. 30 del Codice.

I dati biometrici raccolti, cifrati e "incorporati" all'interno del documento informatico, sarebbero conservati, nei limiti delle finalità indicate, per il periodo di tempo stabilito dalle disposizioni vigenti (art. 2220 cod. civ.; art. 119 del d.lgs. n. 385/1993), fatta salva l'esigenza di una loro ulteriore conservazione in ragione di eventuali contestazioni in sede giudiziaria.

Nel merito degli ulteriori adempimenti gravanti sul titolare del trattamento, la banca ha dichiarato di aver già provveduto all'aggiornamento (puntualmente riscontrato dall'Ufficio) della notifica a suo tempo effettuata ex art. 37 del Codice, come pure di aver adottato le previste misure di sicurezza a protezione dei dati personali degli interessati (tra cui l'"immediata cifratura delle informazioni biometriche" e l'utilizzo di canali di "comunicazione cifrata"), precisando altresì che la conservazione dei dati da parte di In.TE.SA. S.p.A. avverrà anche in conformità ai requisiti previsti dalla delibera del(l'ormai ex) CNIPA n. 11/2004.

1.4. Il sistema, oltre a garantire maggiore celerità nelle operazioni con i promotori e una riduzione dei costi di gestione e del contenzioso, garantirebbe alla banca di poter correttamente adempiere agli obblighi imposti dalla normativa vigente, avuto particolare riguardo al soddisfacimento del requisito della forma scritta previsto a pena di nullità per i contratti (art. 117 del d.lgs. n. 385/1993 e art. 23 del d.lgs. n. 58/1998). Come già anticipato, infatti, il servizio descritto soddisferebbe, nell'ottica della banca, i requisiti previsti dal Codice dell'amministrazione digitale e dal recente d.P.C.M. del 22 febbraio 2013 in tema di firma elettronica avanzata (con particolare riguardo al requisito della "forma scritta") e si discosterebbe – quanto a caratteristiche del trattamento– dalle soluzioni di firma digitale sinora esaminate dall'Autorità (cfr. Provv. 31

gennaio 2013, cit.), essendo la raccolta dei dati biometrici funzionale a garantire una connessione univoca tra la firma apposta in forma elettronica sul documento e il suo autore.

2. Le valutazioni dell'Autorità.

2.1. La verifica preliminare presentata da Fineco Bank S.p.A. ha ad oggetto il trattamento dei dati personali connesso all'utilizzo di un sistema idoneo a rilevare l'immagine della firma autografa apposta dagli interessati su dispositivi a ciò preposti ("tablet") e ad analizzarne alcuni parametri (pressione; accelerazione; inclinazione; ecc.) in vista della sottoscrizione in formato elettronico di atti, contratti e documenti relativi a prodotti e servizi offerti dalla banca per il tramite dei relativi promotori.

Preliminarmente, occorre ricordare 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 un trattamento di dati biometrici ("grafometrici" nell'accezione utilizzata dalla banca) 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; v. anche Provv. Garante 31 gennaio 2013, cit.).

Ciò premesso, occorre valutare, in tale prospettiva, se il sistema sottoposto al vaglio dell'Autorità possa reputarsi conforme, limitatamente ai profili concernenti il trattamento del tratto grafico della firma e dei dati biometrici degli utenti, 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).

2.2. A tale proposito, vale sottolineare che il trattamento dei dati personali (anche biometrici) che la società intende effettuare, in base alla documentazione prodotta e alle dichiarazioni rese anche ai sensi dell'art. 168 del Codice, risulta lecito.

Premesso, infatti, che il trattamento dell'immagine della firma apposta sui "tablet" non risulta connotato, ancorché effettuato con strumenti elettronici, da specifici ed evidenti rischi per gli interessati (anche in ragione delle misure di sicurezza dichiarate dal titolare e dei rigidi protocolli operativi previsti per legge in capo all'organismo certificatore), occorre poi sottolineare, con specifico riferimento al trattamento dei dati biometrici dei firmatari, che il recente d.P.C.M. 22 febbraio 2013, adottato con il parere favorevole del Garante (v. Provv. 24 novembre 2011, doc. web n. **1870620**), contempla espressamente tali dati tra gli elementi utilizzabili ai fini della generazione della firma elettronica avanzata (art. 56).

A ciò, deve aggiungersi che il trattamento dei predetti dati, effettuato esclusivamente previa acquisizione del libero consenso informato dei firmatari (artt. 13 e 23 del Codice) e per il perseguimento di legittime finalità rese note agli interessati (artt. 11, comma 1, lett. b), del Codice), può risultare effettivamente funzionale, anche a garanzia di questi ultimi, in vista di eventuali contenziosi legati al disconoscimento della sottoscrizione apposta su atti e documenti di tipo negoziale, fornendo possibili elementi di valutazione utili anche in sede giudiziaria.

Ciò, correlativamente al fatto che l'utilizzo della soluzione proposta potrebbe efficacemente contribuire, attraverso la garanzia di autenticità, non ripudio e integrità dei documenti sottoscritti elettronicamente, a conferire maggiore certezza nei rapporti giuridici intercorrenti con gli utenti (nel caso di specie, peraltro, mediati dai promotori finanziari).

Pertanto, nella misura in cui la "firma grafometrica" –anche alla luce di quanto previsto dagli artt. 117 del d.lgs. n. 385/1993 e 23 del d.lgs. n. 58/1998–, possa essere effettivamente ricondotta tra le soluzioni che, a norma di legge (cfr. art. 21 del d.lgs. n. 52/2005), soddisfano il requisito della forma scritta, può ragionevolmente ritenersi che il trattamento di dati personali (anche biometrici) connesso al servizio in esame –che asseconda, indubbiamente, legittime esigenze organizzative della società–, ove effettuato con le modalità indicate e nei limiti delle finalità dichiarate, non sia in violazione dei principi di cui all'art. 11, comma 1, lett. a) e b), del Codice; tanto, muovendo dall'ulteriore considerazione che il sistema risulta anche conforme alle "specifiche tecniche" stabilite dall'ISO –nel caso di specie relative ai requisiti previsti per la gestione della sicurezza informatica: ISO/IEC27001:2005– già ritenute rilevanti dal Garante anche sotto il profilo della disciplina di protezione dei dati personali (cfr. Provv. 14 luglio 2011, doc. web n. **1836335**; Provv. 26 maggio 2011, doc. web n. **1832558**; Provv. 2 dicembre 2010, doc. web n. **1779678**) .

Per quanto attiene, poi, all'osservanza dei princìpi di necessità e proporzionalità (artt. 3 e 11, comma 1, lett. d), del Codice), il sistema descritto, nelle modalità di configurazione indicate –tali cioè, secondo la società, da non consentire, in nessun caso, l'acquisizione di informazioni relative allo stato di salute degli interessati–, risulta predisposto per raccogliere un numero circoscritto di informazioni (tassativamente indicate ne: l'immagine della firma; il ritmo; la velocità; la pressione; l'accelerazione; il movimento), allo stato non eccedenti o ultronee rispetto alle finalità dichiarate dalla società. Inoltre, i dati biometrici non saranno accessibili "in chiaro" al titolare se non nei casi previsti e su espressa richiesta dell'autorità giudiziaria.

Sotto il profilo della sicurezza dei dati trattati, si può ritenere che l'insieme degli accorgimenti adottati nell'intero processo di gestione dei dati biometrici degli interessati costituiscano, nel complesso, misure di sicurezza che, sulla base delle attuali conoscenze, possono essere ritenute idonee.

In particolare, si ritiene adeguato il fatto che la società deputata all'emissione dei certificati di firma e di cifratura sia un ente certificatore accreditato presso AgID ex art. 29 CAD e che la chiave privata e il relativo codice di sblocco associati al certificato di sicurezza Fineco, utilizzato per la cifratura dei dati biometrici, siano sempre tenuti separati, scongiurando

così la possibilità di procedere alla decifratura del dato biometrico se non nei casi in cui si renda necessaria una perizia disposta dall'Autorità giudiziaria.

Fermo restando quanto appena detto, si ritiene comunque opportuno, in assenza di indicazioni in tal senso da parte del titolare, indicare ulteriori misure e accorgimenti volti a rafforzare la sicurezza del processo a garanzia degli interessati.

In effetti, la riservatezza dei dati biometrici durante la fase di raccolta si basa, oltre che sulla robustezza della procedura, anche sulla sicurezza dei dispositivi, aspetto sul quale la banca dovrà porre la massima attenzione garantendone l'uso esclusivo ai soli utenti (promotori finanziari) abilitati al relativo utilizzo.

A tale proposito, dovranno essere adottate, ove non ancora previste, idonee misure volte a ridurre i rischi di installazione abusiva di software o di modificazione della configurazione dei dispositivi in dotazione ai promotori, adottando altresì ogni accorgimento utile a contrastare l'azione di eventuali agenti malevoli (malware). Qualora non si sia già provveduto, andrà inoltre adottato un sistema di gestione dei dispositivi impiegati nei trattamenti grafometrici basato su certificazioni digitali e policy di sicurezza che disciplinino, sulla base di criteri predeterminati, le condizioni di loro utilizzo sicuro; in particolare, dovranno risultare disponibili funzionalità di remote wiping applicabili nei casi di smarrimento o sottrazione dei dispositivi. La banca dovrà altresì prevedere adeguate policy per la gestione degli incidenti di sicurezza nell'ambito delle diverse fasi del processo biometrico/grafometrico.

Ancora, risulta adeguata, per altro verso, la prospettata designazione dei promotori finanziari quali incaricati del trattamento, nella misura in cui la banca –previa rinnovata valutazione– non ritenga invece sussistenti, con riferimento al ruolo concretamente svolto da costoro, i presupposti di cui agli artt. 4, comma 1, lett. f) e g), 28 e 29 del Codice.

La società, infine, potrà conservare i dati personali (anche biometrici) tratti dalla firma apposta sui tablet non oltre il termine previsto per la conservazione dell'atto o del documento cui la firma si riferisce (art. 11, comma 1, lett. e), del Codice), fatta salva l'eventuale esigenza di una loro ulteriore conservazione in ragione di specifiche disposizioni di legge o per la tutela di un diritto in sede giudiziaria.

Resta inteso che, in base alla regola n. 25 del disciplinare tecnico in materia di misure minime di sicurezza, la società dovrà farsi rilasciare dall'installatore il previsto attestato di conformità, da conservarsi a cura del titolare medesimo.

Parimenti, resta inteso che la liceità del trattamento resta subordinata all'effettiva osservanza di tutti gli obblighi che la società, nel corso del procedimento, si è impegnata a rispettare (punto 1.3) e di quelli ulteriori eventualmente gravanti sulla base della disciplina vigente (in tal senso, peraltro, appare dirimente la circostanza che il servizio di firma "grafometrica" che la banca intende utilizzare nei rapporti –mediati– con i propri clienti risulti effettivamente riconducibile, come dalla stessa dichiarato, nell'ambito della c.d. "firma elettronica avanzata", prevista e disciplinata dai già citati d.lgs. 7 marzo 2005, n. 82 e d.P.C.M. 22 febbraio 2013).

TUTTO CIÒ PREMESSO IL GARANTE

ai sensi degli artt. 17 e 154 del Codice e a conclusione del relativo iter procedimentale, accoglie l'istanza di verifica preliminare presentata da Fineco Bank S.p.A. e, per l'effetto, ammette il trattamento dei dati personali (anche biometrici) connesso all'utilizzo del sistema descritto, a condizione che:

– esso venga effettuato con le modalità indicate in narrativa e per le sole finalità dichiarate;

– la società, qualora non vi abbia già provveduto, adotti gli ulteriori presidi tecnici e organizzativi di sicurezza a protezione dei dati biometrici degli interessati descritti al precedente punto 2.2 e, segnatamente:

- idonee misure volte a ridurre i rischi di installazione abusiva di software o di modificazione della configurazione dei dispositivi in dotazione ai promotori, adottando altresì ogni accorgimento utile a contrastare l'azione di eventuali agenti malevoli (malware);

- un sistema di gestione dei dispositivi impiegati nei trattamenti grafometrici basato su certificazioni digitali e policy di sicurezza che disciplinino, sulla base di criteri predeterminati, le condizioni di loro utilizzo sicuro. In particolare, dovranno risultare disponibili funzionalità di remote wiping applicabili nei casi di smarrimento o sottrazione dei dispositivi;

- adeguate policy per la gestione degli incidenti di sicurezza nell'ambito delle diverse fasi del processo biometrico/grafometrico;

– la società si faccia rilasciare e conservi l'attestato di conformità di cui alla regola 25 dell'Allegato "B" al Codice;

– la società osservi effettivamente tutti gli obblighi che, nel corso del procedimento, si è impegnata a rispettare (punto 1.3) e quelli ulteriori eventualmente gravanti sulla base della disciplina vigente.

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, 12 settembre 2013

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia