[vedi anche newsletter del 6 marzo 2014]

[doc. web n. 2938921]

Servizio di firma digitale remota con autenticazione biometrica. Verifica preliminare richiesta da Telecom Italia Trust Technologies s.r.l. e Banca Generali S.p.A. - 23 gennaio 2014

Registro dei provvedimenti
n. 25 del 23 gennaio 2014

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";

VISTA la richiesta di verifica preliminare presentata da IT Telecom s.r.l. (oggi Telecom Italia Trust Technologies s.r.l.) e da Banca Generali S.p.A. ai sensi dell'art. 17 del Codice, nonché le successive comunicazioni inviate dalle due società;

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. Il servizio di firma digitale remota con autenticazione biometrica.

1.1. Telecom Italia Trust Technologies s.r.l. e Banca Generali S.p.A., con nota congiunta presentata in data 8 febbraio 2013 – successivamente regolarizzata con distinte comunicazioni del 19 aprile e del 21 giugno 2013– hanno presentato a questa Autorità una richiesta di verifica preliminare ex art. 17 del Codice in merito al trattamento di dati personali connesso all'utilizzo di un sistema di rilevazione delle caratteristiche "dinamiche" della firma apposta dagli utenti in occasione della sottoscrizione di documenti e modulistica bancaria con firma digitale. Si tratterebbe, in sostanza, di un servizio in grado di riconoscere le caratteristiche "comportamentali" dell'interessato attraverso l'analisi di alcuni parametri (velocità del gesto; pressione; accelerazione; inclinazione; ecc.) desumibili dalla firma autografa apposta da quest'ultimo su appositi dispositivi ("tablet") resi disponibili ai promotori finanziari della banca in vista della relativa autenticazione e del contestuale avvio delle procedure per la sottoscrizione dei documenti con firma digitale. Tale servizio, reso a vantaggio della banca e dei relativi clienti da Telecom Italia S.p.A. (per il tramite di Telecom Italia Trust Technologies s.r.l., nella sua qualità di ente certificatore accreditato presso l'Agenzia per l'Italia Digitale), consterebbe, in base alla documentazione trasmessa, di due distinte fasi.

1.2.1. In una prima fase ("provisioning"), l'utente che intendesse avvalersi del servizio, previa identificazione da parte del promotore e "registrazione" dei suoi dati anagrafici nei sistemi informativi della banca, apporrebbe "sul tablet la propria firma autografa almeno tre volte", sì da generare il relativo "specimen" da utilizzare quale termine di "raffronto" nelle successive sessioni di autenticazione; tale specimen, costituito dalle rappresentazioni digitali sintetiche (template) generate in occasione della raccolta delle firme autografe (e contenenti le caratteristiche "biometriche" delle stesse), sarebbe memorizzato in un apposita base di dati –distinta da altri clienti– adeguatamente custodita presso Telecom Italia Trust Technologies s.r.l. Nell'ambito di tale fase, lo specimen, unitamente ai dati identificativi dell'interessato, verrebbe trasmesso dalla banca, in modalità cifrata e attraverso canali dichiaratamente sicuri, alla certification authority per la verifica e convalida della richiesta e per l'emissione del certificato digitale associato al richiedente, che provvederebbe a sua volta a concludere la procedura sottoscrivendo l'apposito modulo contenente anche le condizioni generali di utilizzo del servizio.

L'intera operazione, sottoscritta digitalmente dal promotore finanziario (a conferma degli adempimenti richiestigli), sarebbe preceduta dal rilascio della prevista informativa al firmatario e dall'acquisizione del consenso al trattamento dei suoi dati personali.

1.2.2. Nella successiva fase di autenticazione, l'utente verrebbe invitato, di volta in volta, ad apporre la propria firma autografa sul tablet in vista dell'attivazione della procedura di sottoscrizione della documentazione con firma digitale; le informazioni acquisite, immediatamente convertite in template, verrebbero trasmesse in modalità cifrata, unitamente all'"impronta" del documento da firmare digitalmente e all'identificativo numerico del firmatario, ad un apposito server ubicato presso l'organismo certificatore. Tale server, al fine di autenticare l'utente, verificherebbe la rispondenza del template acquisito con quello memorizzato nel database all'atto della "registrazione", accertando che il numero seriale del tablet sia effettivamente tra quelli censiti. Inoltre, al fine di scongiurare utilizzi fraudolenti del servizio, verrebbe memorizzato (in maniera non collegata al firmatario) anche l'"hash" del template, onde verificarne l'eventuale correlazione con uno degli "hash" dei template già acquisiti in occasione di precedenti operazioni di firma poste in essere dal medesimo firmatario (in tal senso, una loro eventuale analogia potrebbe risultare sintomatica di presunte anomalie). L'operazione di autenticazione si concluderebbe positivamente solo se tutte e tre le verifiche (le prime due con esito affermativo, la terza con esito negativo) saranno andate a buon fine.

Secondo quanto riferito, nessun dato biometrico verrebbe salvato all'esito del confronto, risultando conservato dall'ente certificatore, per ciascuna operazione compiuta, solamente l'hash di riferimento in vista delle successive attività di verifica (cfr. e-mail dell'11 luglio 2013). Inoltre, l'operazione di autenticazione non risulterebbe inficiata dalla modificabilità nel tempo dello stile di firma degli utenti, considerata la potenziale idoneità del sistema ad auto-aggiornare lo specimen sulla base di regole fondate "su elementi temporali, numerici e statistici" e la possibilità –comunque riconosciuta ai firmatari– di sostituirlo con nuovi specimen. Infine, i dati biometrici acquisiti dal sistema (il cui grado di affidabilità sarebbe stato testato da laboratori considerati indipendenti) verrebbero trattati secondo gli specifici standard attualmente vigenti (ISO/IEC 19794-7).

Il supporto nella gestione tecnica dei dispositivi e la relativa configurazione sarebbero affidati, nell'interesse della banca, a una società terza (Xenesys s.r.l.).

1.3. In base alle dichiarazioni rese, l'intero processo di autenticazione, ancorché prodromico a quello concernente l'apposizione della firma digitale, dovrebbe ritenersi distinto da quest'ultimo, preordinato alla sottoscrizione elettronica dei documenti attraverso la chiave privata del firmatario associata al certificato digitale custodito presso l'Hardware Security Module gestito dall'ente certificatore. Le componenti architetturali coinvolte nel servizio, infatti, sarebbero "state predisposte in modo tale che i dati biometrici siano trattati esclusivamente dai sistemi utilizzati per l'autenticazione forte […] e non dai sistemi coinvolti nei processi di rilascio dei certificati qualificati […], ovvero delle procedure richieste per l'apposizione della firma digitale". Ne deriva che i dati biometrici degli utenti verrebbero trattati, a fini di autenticazione, esclusivamente attraverso il server a ciò dedicato (autonomo e separato da quelli impiegati per il rilascio dei certificati digitali e per l'apposizione della firma digitale), al pari dei dati identificativi degli interessati, anch'essi archiviati presso un server distinto da quello previsto per la memorizzazione (in modalità cifrata) degli specimen per evitare la loro diretta e immediata associabilità. Gli stessi server, inoltre, verrebbero ubicati in locali protetti e accessibili ai soli soggetti a ciò legittimati in ragione delle mansioni svolte, mentre le operazioni sui dati e sui sistemi verrebbero adeguatamente tracciate attraverso un apposito sistema di "access & audit logging". Infine, i dispositivi in dotazione ai promotori –già dotati di antivirus periodicamente aggiornati e configurati in conformità alle policy (non modificabili, né rimovibili dall'utente) definite secondo il contesto di sicurezza individuato dalla banca– permetterebbero, attraverso le componenti applicative ivi installate e la connessa piattaforma di riferimento (Mobile Device Management), di gestire tempestivamente ipotetici tentativi di manomissione, consentendo l'attivazione delle previste procedure di blocco e di cancellazione selettiva o totale dei contenuti (c.d. wiping); tanto, fermo restando che le informazioni presenti sui "tablet" (che, comunque, non riguardano dati biometrici, nemmeno memorizzati dai dispositivi) non sarebbero accessibili, in ogni caso, mediante collegamenti USB o altre interfacce alternative.

Tali complessive misure, unitamente alla stringente vigilanza cui risulta soggetto il certificatore accreditato anche in merito ai profili relativi alla gestione della sicurezza dei dati e dei sistemi, consentirebbero di ritenere che le informazioni utilizzate nell'ambito della procedura di autenticazione biometrica non sarebbero "direttamente utilizzabili […] in altri contesti con effetti sugli interessati".

1.4. Il trattamento dei dati in esame, secondo quanto riferito, verrebbe svolto dalle società istanti in qualità di autonome titolari. Difatti, muovendo dalla considerazione che l'ente certificatore effettuerebbe "il trattamento dei dati biometrici per la finalità di autenticazione dei firmatari con riferimento alla gestione del proprio servizio di firma digitale" e che la banca tratterebbe tali dati "limitatamente a quanto necessario per acquisire e trasferire gli stessi a [Telecom Italia Trust Technologies s.r.l.]" (secondo modalità autonomamente definite, purché "in coerenza con i requisiti tecnico-operativi stabiliti dal certificatore accreditato"), le società ritengono che "le finalità e gli ambiti di attività [sarebbero] distinti sotto il profilo operativo ed organizzativo, [pur] nell'ambito della fornitura al cliente di un servizio omogeneo, preordinato all'accesso ai servizi bancari e di investimento offerti da Banca Generali per il tramite del servizio di firma digitale di" Telecom Italia Trust Technologies s.r.l. Correlativamente, in ragione di tale ritenuta autonoma titolarità, sia la banca che l'ente certificatore risultano aver predisposto due distinti testi di informativa da sottoporre agli interessati antecedentemente all'attivazione del servizio (e all'avvio del connesso trattamento), approntando anche due diversi moduli per l'acquisizione del relativo consenso. Per contro, nessun trattamento di dati biometrici sarebbe effettuato da Telecom Italia S.p.A., operando quest'ultima quale semplice distributore dei servizi concretamente erogati da Telecom Italia Trust Technologies s.r.l.

Per quanto attiene agli altri adempimenti che la normativa vigente pone in capo ai titolari dei trattamenti, ferma restando la necessaria modifica alle notifiche già effettuate, risulta agli atti che la banca avrebbe intenzione di designare i promotori finanziari detentori dei "tablet" quali incaricati ai sensi dell'art. 30 del Codice, provvedendo altresì all'integrazione della nomina a responsabile esterno del trattamento nei confronti della società consortile deputata alla fornitura e gestione dei servizi informativi nell'interesse della banca medesima. Parimenti, l'ente certificatore provvederebbe a designare i soggetti preposti esclusivamente ai servizi di certificazione (peraltro esigui nel numero) quali incaricati del trattamento.

Nessuna indicazione, per contro, è stata fornita con riferimento al ruolo (sotto il profilo privacy) di Xenesys s.r.l., chiamata a gestire tecnicamente i dispositivi, nell'interesse della banca, sulla base di un accordo intercorso con quest'ultima.

1.5. Il sistema, nel suo complesso, verrebbe utilizzato dall'istituto di credito per conferire maggiore certezza e sicurezza alle operazioni effettuate dagli utenti (nel caso di specie, peraltro, mediate dai promotori finanziari), garantendo, attraverso l'utilizzo del dato biometrico a fini di autenticazione, l'effettiva riconducibilità della sottoscrizione e del documento al firmatario (rigorosamente identificato) e assicurando, in pari tempo, una sensibile riduzione del rischio legato al fenomeno dei furti di identità. Lo stesso sistema, inoltre, verrebbe impiegato nella prospettiva di apportare significativi miglioramenti ai processi organizzativi e gestionali della banca, in termini soprattutto di "efficienza"

(semplificazione e snellimento delle operazioni effettuate per il tramite dei promotori finanziari; incremento della qualità dei servizi resi) ed "economicità delle risorse" (dematerializzazione della modulistica; riduzione dei costi di conservazione dei documenti; rispetto per l'ambiente).

Per contro, i dati personali (anche biometrici) degli utenti verrebbero trattati dall'ente certificatore, nel rispetto degli standard operativi ed organizzativi imposti dalla normativa di settore, esclusivamente ai fini dell'attivazione ed erogazione del servizio, nei limiti e con le modalità convenute con la banca e stabilite nelle apposite condizioni contrattuali.

2. Le valutazioni dell'Autorità.

2.1. 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 di documenti con firma digitale. Il presente provvedimento, che tiene conto del tenore dell'istanza formulata e delle dichiarazioni rese dalle parti (anche ai sensi dell'art. 168 del Codice), si sofferma sui soli profili relativi al trattamento dei dati personali biometrici effettuato nella fase di autenticazione.

Come già evidenziato da questa Autorità (cfr. Provv. 31 gennaio 2013, docc. web nn. 2304808 e 2311886), occorre anzitutto muovere dalle considerazioni già espresse dal Gruppo per la tutela dei dati personali ex art. 29 della direttiva 95/46/Ce, secondo cui l'utilizzo di sistemi basati sull'impiego di dispositivi in grado di rilevare le caratteristiche "dinamiche" della firma determina, 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, nella prospettiva evidenziata, se il sistema sottoposto al vaglio dell'Autorità possa reputarsi conforme, limitatamente ai profili concernenti il trattamento di dati biometrici degli utenti nella fase di autenticazione, alla disciplina del Codice, con particolare riferimento sia alla corretta identificazione del ruolo rivestito dalle società coinvolte nell'ambito della procedura di autenticazione, sia 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 dalla banca, come nel caso in esame, ai soli fini del completamento della fase di enrollment e venga successivamente utilizzato (sotto forma di codice numerico), da parte del certificatore accreditato, per le operazioni di raffronto nell'ambito delle 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).

2.2. Rispetto al primo profilo, gli elementi acquisiti inducono a ritenere che, diversamente da quanto sostenuto dalle società istanti, debba essere privilegiata, anche alla luce del peculiare assetto contrattuale prescelto dalle parti, l'ipotesi di una contitolarità del medesimo (e unico) trattamento di dati biometrici (art. 4, comma 1, lett. f), del Codice).

Muovendo dalle valutazioni espresse dal menzionato Gruppo per la tutela dei dati personali –secondo cui "si è in presenza di una situazione di corresponsabilità quando varie parti determinano, per specifici trattamenti, o la finalità o quegli aspetti fondamentali degli strumenti […]. Nel contesto della corresponsabilità, comunque, la partecipazione delle parti alla determinazione congiunta può assumere varie forme e non deve essere necessariamente ripartita in modo uguale", potendo i vari titolari "occuparsi –e quindi rispondere– del trattamento di dati personali in fasi diverse e a gradi diversi" (così Parere 1/2010 sui concetti di titolare e incaricato del trattamento, WP 169, adottato il 16 febbraio 2010, p. 19; per alcune pronunce in tal senso, v. Provv. Garante 3 dicembre 2009, doc. web n. 1692917; Provv. 30 maggio 2007, doc. web n. 1412610; Provv. 13 settembre 2012, doc. web n. 1927456)–, si rileva che il servizio in esame, reso attraverso l'utilizzo in forma "integrata" delle piattaforme informative della banca e di Telecom Italia Trust Technologies s.r.l., risponde anzitutto all'esigenza –comune ad entrambe le parti– di garantire, nel rispetto delle rispettive discipline di settore, certezza e sicurezza alle operazioni intercorrenti con gli utenti. In tale ottica, non può non rilevarsi che:

– Telecom Italia S.p.A.: non assume alcun ruolo effettivo nell'attivazione ed esecuzione della procedura di autenticazione, né tratta, in concreto, dati biometrici riferibili agli interessati;

– Banca Generali S.p.A.:

- determina le finalità del trattamento, richiedendo nel proprio interesse (cfr. la "lettera di intenti" del 16 gennaio 2013, nonché le "condizioni di utilizzo del servizio di firma digitale biometrica" emesse in data 24 maggio 2013; v. anche l'informativa presente sul modulo per la richiesta di attivazione del servizio) l'erogazione del complessivo servizio (comprensivo del trattamento dei dati biometrici a fini di autenticazione) concretamente fornito da Telecom Italia Trust Technologies s.r.l. a vantaggio dei firmatari che intendano avvalersene;
- delimita i "confini" di utilizzabilità del servizio medesimo, circoscrivendoli alla sola modulistica bancaria o di interesse bancario;
- determina, in coerenza con i requisiti tecnico-operativi stabiliti dall'ente certificatore, le modalità di esecuzione del trattamento e le misure di sicurezza, limitatamente alle operazioni di raccolta dei dati biometrici degli interessati;
- concorda con l'ente certificatore, nel rispetto delle previsioni di legge, le procedure operative per l'identificazione e registrazione dei firmatari;
- vanta poteri di controllo e verifica in merito alle "prestazioni" concretamente erogate dalla certification authority;

– Telecom Italia Trust Technologies s.r.l.:

- determina (in armonia con le esigenze della banca) le finalità del trattamento, rapportandole alla gestione del complessivo servizio di firma digitale fornito all'istituto;

- determina le modalità di esecuzione del trattamento, definendo gli standard tecnici e organizzativi della procedura di autenticazione anche in adempimento alle specifiche disposizioni di settore;

- concorda con la banca le procedure operative per l'identificazione e registrazione dei firmatari;

- apporta, sulle modalità di erogazione del servizio, le eventuali modifiche richieste dall'evoluzione tecnologica e normativa (cfr. le citate condizioni di utilizzo del servizio, p. 3);

- adotta, nell'ambito del complessivo servizio di sottoscrizione con firma digitale (cui il trattamento di dati biometrici è preordinato), le misure necessarie all'organizzazione del medesimo, ivi comprese le misure di sicurezza di cui alla disciplina del Codice (cfr. il Manuale operativo di Telecom Italia Trust Technologies s.r.l.).

Alla luce di tali complessivi elementi, appare arduo, nel caso di specie, ipotizzare due distinti trattamenti di dati biometrici in capo alla banca e a Telecom Italia Trust Technologies s.r.l. (i quali, peraltro, autonomamente considerati, risulterebbero fini a sé stessi), dovendo piuttosto ritenersi, anche in vista di un più agevole esercizio dei diritti di cui all'art. 7 del Codice da parte degli interessati, che le società coinvolte, ancorché operanti "in sequenza", pongano in essere –nell'ambito di un servizio definito "omogeneo" dalle stesse parti istanti (v. nota del 21 giugno 2013, p. 3)– operazioni differenti di un unico trattamento preordinato all'autenticazione degli interessati, avvalendosi a tal fine di strumenti stabiliti congiuntamente (e operanti in forma "integrata") e rispondendo del medesimo trattamento solo per la parte di propria competenza (in tal senso, v. anche il menzionato parere del Gruppo art. 29, p. 21). Tale impostazione trova riscontro anche nelle richiamate "condizioni di utilizzo del servizio di firma digitale biometrica", secondo cui "il trattamento […] è diretto esclusivamente all'espletamento da parte della banca e di [Telecom Italia Trust Technologies s.r.l.], in qualità di co-titolari del trattamento e nell'ambito delle rispettive competenze ed attività, […]".

2.3. Per quanto attiene all'osservanza dei princìpi stabiliti dal Codice, vale evidenziare che il trattamento dei dati biometrici che le società istanti intendono effettuare, in base alla documentazione prodotta e alle dichiarazioni rese, risulta lecito.

Al riguardo, occorre anzitutto sottolineare che l'utilizzabilità dei dati biometrici nell'ambito delle procedure di firma di documenti informatici è espressamente prevista dal 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".

Si deve poi prendere atto, in termini più generali, della crescente considerazione che, anche a livello europeo, sta acquisendo l'utilizzo di dati biometrici a fini di autenticazione, soprattutto in ragione delle ritenute garanzie di affidabilità che tali dati offrirebbero –a fortiori nel peculiare contesto bancario, notoriamente esposto al rischio di frodi (v. infra)– sul piano della rigorosa identificabilità degli utenti e, correlativamente, dell'effettiva riconducibilità a questi ultimi delle operazioni effettuate (cfr. Recommendation for the security payments, Banca Centrale Europea, aprile 2012; sul piano nazionale, v. "Attuazione del Titolo II del decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento (Diritti ed obblighi delle parti) – Allegato Tecnico «Tipologie di strumenti di più elevata qualità sotto il profilo della sicurezza»", Banca d'Italia, 5 luglio 2011; "Documento per la consultazione – Disposizioni di Vigilanza prudenziale per le banche – Sistema dei controlli interni, sistema informativo e continuità operativa", Banca d'Italia, 4 settembre 2012). Correlativamente, non va sottaciuto il beneficio che anche gli enti certificatori –già tenuti, in ragione delle proprie numerose responsabilità, ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno a terzi (cfr. art. 32 del d.lgs. n. 82/2005, cit.)– potrebbero trarre (in termini, soprattutto, di maggiore affidabilità delle operazioni di autenticazione effettuate dai firmatari) dall'utilizzo di tali dati nell'ambito dell'apposito servizio qui considerato.

Occorre poi sottolineare che il trattamento in esame potrebbe, da un lato, effettivamente contribuire, nel delicato contesto bancario, a contrastare in maniera efficace il fenomeno criminoso dei furti di identità –conferendo, quindi, maggiore certezza e sicurezza nei rapporti giuridici intercorrenti con gli utenti (peraltro mediati, nel caso di specie, da soggetti terzi)– e, dall'altro, a snellire e velocizzare, anche a vantaggio della stessa clientela, le operazioni effettuate per il tramite dei promotori finanziari. Considerato, infine, che i dati biometrici sarebbero raccolti con il consenso degli interessati e per legittime finalità rese note a questi ultimi, si può ragionevolmente ritenere –nella misura in cui il sistema risulti effettivamente conforme al quadro normativo vigente (d.lgs. n. 82/2005, cit.; d.P.C.M. 22 febbraio 2013, cit.), anche sul piano delle relative certificazioni di sicurezza– che il trattamento in questione soddisfi i requisiti di cui all'art. 11, comma 1, lett. a) e b), del Codice.

Per quanto attiene, poi, all'osservanza dei princìpi di necessità e proporzionalità (artt. 3 e 11, comma 1, lett. d), del Codice), risulta che il sistema descritto, nelle modalità di configurazione indicate, consente di trattare i dati biometrici degli interessati in forma "disgiunta" dai relativi dati anagrafici (memorizzati in un apposito database, peraltro distinto da quello contenente gli specimen), sì da permettere la loro identificazione solo indirettamente. Inoltre, le informazioni biometriche acquisite dal sistema risultano essere solo quelle necessarie alla creazione del template e alle successive operazioni di raffronto in sede di autenticazione degli interessati.

Anche le misure di sicurezza indicate –fatto salvo quanto precisato al successivo punto 3– appaiono tali, allo stato della tecnica, da far ritenere come remoto il rischio di trattamento indebito dei dati biometrici degli interessati (art. 31 e ss.).

Si prende atto, infine, che il sistema sarebbe in grado, attraverso un meccanismo di auto-apprendimento, di garantire nel tempo la "qualità" dei dati biometrici trattati (art. 11, comma 1, lett. c), del Codice).

3. Ulteriori adempimenti.

Le società istanti hanno dichiarato che, antecedentemente all'inizio del trattamento, provvederanno a fornire agli interessati la prevista informativa comprensiva di tutti gli elementi di cui all'art. 13 del Codice; tale informativa dovrà essere opportunamente modificata nella parte relativa al profilo della co-titolarità del trattamento (secondo quanto precisato al precedente punto 2.2.), precisando meglio, ex latere banca, le finalità del trattamento medesimo (cfr. punto 1.5), allo stato indicate solo genericamente ("al fine di permettere l'accesso al servizio Firma Sicura Biometrica"). Parimenti, dovrà essere opportunamente emendata (o meglio precisata), perché potenzialmente fuorviante, la modulistica concernente la "richiesta di attivazione del servizio di «firma sicura biometrica»", da cui risulta che "[…] il confronto, la conseguente conservazione dei dati biometrici e, in generale, l'apposizione della firma digitale avverranno a cura di Telecom Italia S.p.A." (sia pure nella sua veste di parte contrattuale).

I dati biometrici degli interessati, inoltre, non potranno essere conservati per un periodo di tempo superiore agli scopi per i quali gli stessi sono stati raccolti e successivamente trattati (art. 11, comma 1, lett. e), del Codice). In particolare, gli specimen raccolti quale termine di raffronto per le successive operazioni di autenticazione potranno essere conservati per il solo periodo di tempo strettamente correlato alla durata del servizio, dopodiché dovranno essere cancellati, sia pure nel rispetto dei tempi tecnici a tal fine necessari. Resta salva, ovviamente, la necessità di una loro ulteriore conservazione in ragione di specifiche previsioni di legge o per la tutela di un diritto in sede giudiziaria.

Infine, non risultando agli atti quale sia la qualifica (sotto il profilo privacy) attribuita a Xenesys s.r.l., si ritiene che la stessa debba essere formalmente designata, anche alla luce del delicato incarico conferitole (rilevante anzitutto sotto il profilo della sicurezza dei dati e dei dispositivi), quale responsabile del trattamento ex artt. 4, comma 1, lett. g) e 29 del Codice.

Resta inteso che il trattamento dei dati biometrici degli interessati potrà essere effettuato, nell'ambito delle procedure in esame, solo previo adempimento all'obbligo di modifica della notificazione già effettuata in conformità agli artt. 37 e ss. del Codice.

Considerata l'utilizzabilità "in mobilità" dei dispositivi in uso ai promotori, si richiama l'attenzione sulla necessità che il trattamento dei dati biometrici degli utenti venga effettuato in rigorosa osservanza delle misure di sicurezza indicate, avuto precipuo riguardo a quelle preordinate a ridurre al minimo i rischi di installazione di software non autorizzati o di contatto con agenti malevoli (malware); inoltre, dovrà essere garantita la funzionalità di remote wiping –già prevista nell'eventuale ipotesi di manomissione– anche in caso di loro smarrimento o sottrazione.

L'installazione di applicazioni dall'app store potrà avvenire esclusivamente per le app preventivamente incluse nel perimetro di sicurezza della piattaforma MDM a seguito di una valutazione della loro conformità alle policy adottate dai titolari del trattamento, scongiurando la possibilità di installazione autonoma di arbitrarie applicazioni da parte degli utilizzatori. Sistemi software di base e applicazioni, inoltre, andranno mantenuti costantemente aggiornati per prevenire lo sfruttamento di eventuali vulnerabilità informatiche.

Ancora, il trattamento dovrà avvenire con modalità sempre rispettose, in concreto, dei diritti e delle libertà fondamentali, nonché della dignità degli interessati (art. 2, comma 1, del Codice) e dovrà essere svolto nel rispetto delle altre discipline di legge eventualmente applicabili (art. 11, comma 1, lett. a) del medesimo Codice). Inoltre, i dati biometrici dei firmatari –che si assumono insuscettibili di utilizzo in altri contesti– non potranno essere impiegati in operazioni di trattamento incompatibili con le finalità originarie della raccolta (art. 11, comma 1, lett. b), del Codice).

Naturalmente, il consenso che le società intendono acquisire potrà considerarsi realmente libero (art. 23 del Codice) solo ove raccolto in assenza di eventuali pressioni o condizionamenti, anche in occasione dell'adesione al servizio (nello stesso senso, già Provv. 31 gennaio 2013, cit.). In tal senso, appare determinante la circostanza che venga realmente rimessa, in capo ai singoli interessati, l'effettiva facoltà di scelta in ordine alla possibilità di avvalersi o meno della procedura di autenticazione biometrica, come pure la possibilità di assicurare comunque la fruizione del servizio di sottoscrizione dei documenti con firma digitale attraverso modalità alternative di autenticazione.

TUTTO CIÒ PREMESSO, IL GARANTE

a conclusione della verifica preliminare richiesta congiuntamente da Banca Generali S.p.A. e Telecom Italia Trust Technologies s.r.l., 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, prescrive, ai sensi dell'art. 17 del Codice, di:

1) modificare l'informativa da rendere agli interessati nella parte relativa al profilo della co-titolarità del trattamento dei dati biometrici (punto 2.2.), precisando meglio, ex latere banca, le finalità del trattamento medesimo (punto 1.5) (art. 13 del Codice);

2) emendare la modulistica concernente la "richiesta di attivazione del servizio di «firma sicura biometrica»", precisando che il soggetto che compie, in concreto, le operazioni relative a "il confronto, la conseguente conservazione dei dati biometrici e, in generale, l'apposizione della firma digitale" è Telecom Italia Trust Technologies s.r.l.;

3) acquisire un consenso realmente libero da parte dei firmatari, in aderenza a quanto disposto dall'art. 23 del Codice;

4) conservare i dati biometrici degli interessati (e, in particolare, gli specimen raccolti quale termine di raffronto per le successive operazioni di autenticazione) per il periodo di tempo indicato (punto 3), fatte salve le esigenze di ulteriore conservazione ivi richiamate (art. 11, comma 1, lett. e), del Codice);

5) designare Xenesys s.r.l. responsabile del trattamento (artt. 4, comma 1, lett. g) e 29 del Codice);

6) modificare, prima dell'inizio del trattamento, le notifiche già effettuate in conformità agli artt. 37 e ss. del Codice;

7) attenersi alle modalità di trattamento rappresentate, rispettando scrupolosamente le misure di sicurezza indicate a tutela dei dati e dei sistemi (cfr. punti 1.3 e 3).

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, 23 gennaio 2014

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia