GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

[doc. web n. 2311886]

Sistemi di rilevazione biometrica. Verifica preliminare richiesta da IT Telecom s.r.l. e Cassa di Risparmio di Parma e Piacenza S.p.A. - 31 gennaio 2013

Registro dei provvedimenti
n. 36 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.lgs. 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali (di seguito "Codice");

VISTA la richiesta di verifica preliminare presentata da IT Telecom s.r.l. e da Cassa di Risparmio di Parma e Piacenza S.p.A. (nella qualità di capogruppo del Gruppo Cariparma Crédit Agricole) ai sensi dell'art. 17 del Codice;

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 dalle società.

1.1. IT Telecom s.r.l. e Cassa di Risparmio di Parma e Piacenza S.p.A., con nota congiunta del 27 aprile 2012 –successivamente regolarizzata, anche nell'interesse di Banca Popolare Friuladria S.p.A. e Cassa di Risparmio della Spezia S.p.A., con comunicazione del 29 novembre 2012– hanno manifestato l'intenzione di voler, rispettivamente, fornire e utilizzare un servizio di firma digitale remota con autenticazione biometrica "basato sull'utilizzo di dispositivi che consentono di rilevare le caratteristiche dinamiche distintive della firma autografa" apposta dagli utenti in occasione della sottoscrizione con firma digitale di contratti o di modulistica bancaria; ciò, al fine di garantire a costoro, attraverso sistemi di "strong authentication", "l'uso delle proprie chiavi private [necessarie] per effettuare operazioni di firma digitale" allo sportello. Si tratterebbe, in sostanza, di un sistema basato su dispositivi sicuri di firma, custoditi da IT Telecom s.r.l. (nella sua qualità di certificatore accreditato presso l'Agenzia per l'Italia Digitale, già DigitPA), in grado di riconoscere le caratteristiche "comportamentali" dell'utente attraverso l'analisi di alcuni parametri desumibili dalla firma autografa (velocità del gesto; pressione; accelerazione; inclinazione; ecc.), apposta da quest'ultimo su un apposito "tablet" presente allo sportello in vista della relativa autenticazione e del contestuale avvio delle procedure per la sottoscrizione dei documenti con firma digitale. Il servizio, fornito concretamente da IT Telecom s.r.l. interfacciandosi con le strutture informatiche disponibili presso le singole banche, comporterebbe un trattamento di dati personali potenzialmente foriero di rischi specifici per gli interessati, ragion per cui le società hanno ritenuto di dover formulare all'Autorità una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice.

A corredo dell'istanza, IT Telecom s.r.l. e Cariparma S.p.A. hanno prodotto due distinti documenti relativi alle modalità di funzionamento del sistema e alle caratteristiche del trattamento che i soggetti coinvolti, per quanto di rispettiva competenza (v. infra), intendono svolgere.

2. Il documento di IT Telecom s.r.l.

2.1. In base alla documentazione inviata da IT Telecom s.r.l., lo schema generale prefigurato per l'espletamento del servizio consta di due fasi.

In una prima fase ("provisioning"), all'utente che intende aderire al servizio, previa identificazione allo sportello e "registrazione" dei suoi dati anagrafici nei sistemi informativi della singola banca, "verrà associato un insieme di informazioni caratteristiche della sua firma autografa (c.d. specimen) rilevate richiedendo al[lo stesso] di apporre sul tablet la propria [sottoscrizione per] almeno tre volte". Lo specimen ottenuto, costituito dalle rappresentazioni digitali sintetiche (template) generate in occasione della raccolta delle firme (contenenti informazioni relative a: l'immagine della firma; l'identificativo del tablet e le caratteristiche "biometriche" della firma autografa), verrà memorizzato in un apposito database custodito presso IT Telecom s.r.l., ai fini delle successive operazioni di raffronto in sede di autenticazione.

Nell'ambito di tale procedura preliminare, lo specimen, unitamente ai dati identificativi dell'interessato, sarà trasmesso dalla banca, in modalità cifrata e attraverso canali dichiaratamente sicuri, a IT Telecom s.r.l. per la verifica e convalida della richiesta e per l'emissione del certificato digitale associato al richiedente.

Il firmatario, previamente informato presso la banca in ordine al trattamento dei suoi dati personali e biometrici in occasione della richiesta di attivazione del servizio –per il quale viene anche acquisito il relativo consenso– provvederà poi a confermare tale richiesta, sottoscrivendo il modulo predisposto da IT Telecom s.r.l. (contenente anche le condizioni generali di utilizzo del servizio).

2.2. Nella successiva fase di autenticazione, l'utente viene invitato, di volta in volta, ad apporre la propria firma autografa sul tablet in vista, tra l'altro, dell'attivazione della procedura di sottoscrizione del documento con firma digitale; le informazioni acquisite, immediatamente convertite in template, vengono trasmesse in modalità cifrata, unitamente all'"impronta" del documento da firmare digitalmente (digest, ottenuto con un algoritmo hash) e all'identificativo numerico del firmatario, ad un apposito server ubicato presso IT Telecom s.r.l. Tale server, al fine di autenticare l'utente, verifica la corrispondenza del template acquisito con quello memorizzato nel database all'atto della "registrazione" e accerta che il numero seriale del tablet sia effettivamente tra quelli censiti. Inoltre, a scopi di sicurezza, viene calcolato anche l'"hash" del template, affinché sia possibile verificarne l'eventuale corrispondenza con uno degli "hash" dei template già verificati in occasione di precedenti operazioni di firma poste in essere dal medesimo firmatario; tale misura ha lo scopo di scongiurare alcuni possibili utilizzi fraudolenti del servizio. L'operazione di autenticazione si concluderà positivamente solo se tutte e tre le verifiche saranno andate a buon fine (in particolare, per poter sbloccare le funzioni di firma digitale, le prime due verifiche dovranno avere esito positivo, mentre la terza dovrà avere esito negativo).

2.3. L'intero processo di autenticazione, a detta della società, deve ritenersi distinto da quello relativo all'apposizione della firma digitale. I dati biometrici degli utenti, infatti, 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; inoltre, i dati identificativi degli utenti verrebbero archiviati presso un server distinto da quello previsto per la memorizzazione (in modalità cifrata) degli specimen, onde evitare la loro diretta e immediata associabilità. Gli stessi server, infine, verrebbero ubicati in locali protetti e accessibili ai soli soggetti a ciò legittimati (incaricati del trattamento e personale specificamente autorizzato da IT Telecom s.r.l.), mentre le operazioni sui dati e sui sistemi verrebbero adeguatamente tracciate attraverso un apposito sistema di "access & audit logging".

Tutto ciò porta la società –sottoposta, in quanto Certification Authority accreditata, alla stringente vigilanza dell'Agenzia per l'Italia Digitale anche in merito ai profili relativi alla gestione della sicurezza dei dati e dei sistemi– ad affermare che le informazioni memorizzate per la verifica biometrica della firma non sarebbero, alla luce delle misure organizzative e gestionali adottate, "direttamente utilizzabili […] in altri contesti con effetti sugli interessati".

Inoltre, i dati biometrici relativi agli utenti, in caso di cessazione del trattamento, verrebbero cancellati o anonimizzati in modalità irreversibile "immediatamente o nei tempi tecnici necessari e comunque non oltre i 30 giorni solari dalla registrazione dell'evento".

2.4. Il sistema, nel suo complesso, oltre a ridurre sensibilmente il rischio di eventuali tentativi di furto di identità, garantirebbe, in prospettiva, la "dematerializzazione dei processi gestiti con documentazione cartacea" per le operazioni da svolgersi direttamente presso gli sportelli bancari. Inoltre, il servizio offerto risponderebbe alla necessità di garantire in capo agli interessati –in osservanza dei vincoli posti dalla normativa in materia di firma digitale– il "controllo esclusivo delle proprie chiavi private di firma ai fini della validità legale dei documenti sottoscritti e della relativa verifica".

3. Il documento di Cariparma S.p.A.

Avvalendosi del sistema in esame, Cariparma S.p.A., al pari di Friuladria S.p.A. e Carispezia S.p.A., ritengono di poter apportare significativi miglioramenti ai propri processi organizzativi e gestionali, soprattutto in termini di "efficienza" (semplificazione e snellimento delle operazioni allo sportello; incremento della qualità dei servizi resi), "sicurezza" (identificazione certa dell'utenza; contrasto alle frodi) ed "economicità delle risorse" (dematerializzazione della modulistica; riduzione dei costi di conservazione dei documenti; rispetto per l'ambiente); ciò, senza alterare significativamente le abitudini degli utenti e sollevando al contempo questi ultimi dall'onere di ricorrere a strumenti addizionali (smart card; token; ecc.) ai fini dell'utilizzo della "chiave privata" di pertinenza, agevolandoli, così, nelle operazioni di sottoscrizione dei documenti con firma digitale.

Nell'ambito di tale complessivo servizio, il trattamento dei dati biometrici risponderebbe principalmente all'esigenza di verificare adeguatamente l'identità degli utenti che abbiano prestato a tal fine il proprio consenso; ciò, non solo in ragione del crescente numero di frodi dichiarato, ma anche in funzione dell'osservanza degli specifici obblighi gravanti sulle singole banche ai sensi della normativa in materia di antiriciclaggio.

Tuttavia, ove gli stessi utenti non potessero o non intendessero avvalersi del servizio di autenticazione biometrica, è stata individuata una modalità "alternativa" che prevede l'utilizzo del telefono cellulare come dispositivo per il riconoscimento dell'interessato, in particolare attraverso l'invio a IT Telecom s.r.l. dell'apposito PIN di firma rilasciato a quest'ultimo dalla medesima certification authority in vista dell'attivazione della procedura di sottoscrizione del documento con firma digitale. Nondimeno, tale ultima modalità dovrebbe ritenersi, a detta delle banche istanti, come "eccezionale", in quanto finalizzata a una "gestione delle attività di sportello difforme da quella collegata all'uso della [firma digitale remota]", che non consentirebbe di realizzare appieno le finalità sopra indicate.

L'attivazione del servizio, ad ogni buon conto, avverrebbe solo dopo il rilascio agli interessati della prevista informativa e dell'acquisizione del relativo consenso al trattamento dei dati biometrici da parte dei rispettivi titolari. Infine, allo scopo di garantire elevati standard di sicurezza in ordine ai dati dell'utenza, le banche istanti hanno dichiarato che gli operatori preposti all'identificazione e alla supervisione delle operazioni di autenticazione biometrica –ritualmente designati incaricati del trattamento ai sensi dell'art. 30 del Codice– potranno trattare i dati personali degli interessati solo previo superamento di un'apposita procedura di autenticazione.

4. Le successive comunicazioni delle società.

Con successive comunicazioni del 20 e 27 novembre e del 21 dicembre 2012, le società istanti hanno fornito alcune precisazioni in ordine al trattamento dei dati biometrici oggetto della richiesta di verifica preliminare, provvedendo, altresì, ad illustrare meglio l'architettura contrattuale prescelta per la fornitura e la fruizione del servizio anche in vista di una più puntuale individuazione, relativamente al

trattamento dei dati biometrici degli interessati, degli effettivi poteri decisionali in capo a ciascuno dei soggetti coinvolti.

Rispetto al primo profilo, nel ribadire la distinzione tra il processo di autenticazione forte e quello di sottoscrizione dei documenti con firma digitale (circostanza, questa, confermata da tutte le parti), IT Telecom s.r.l. ha poi precisato, per parte sua, che il servizio offerto tiene conto della "modificabilità nel tempo della firma autografa" (attraverso funzioni di "auto-apprendimento" che consentirebbero un costante "aggiornamento dello specimen [sulla] base [di] regole [operanti su] elementi temporali, numerici e statistici"), mentre le banche hanno confermato, per quanto di loro spettanza, di voler avvalersi del servizio medesimo, tra l'altro, ai fini di un'"adeguata verifica della clientela richiesta dalla normativa in materia di antiriciclaggio". Inoltre, con specifico riferimento al grado di affidabilità del sistema –già preimpostato al fine di garantire un numero ridotto di eventuali "falsi positivi" e "falsi negativi": c.d. "grado di tolleranza del sistema"–, è stato chiarito che tale rischio deve ritenersi ulteriormente ridotto a fronte delle modalità di organizzazione prescelte per il servizio medesimo, che prevedono il riconoscimento de visu del firmatario da parte dell'incaricato all'identificazione presso la singola banca.

Nell'ambito, poi, del complesso schema prefigurato dalle parti per l'erogazione e la fruizione del servizio –che contempla la stipula di un contratto tra le banche e Telecom Italia S.p.A. (nella sua qualità di distributore "dei servizi di certification authority" subappaltati a IT Telecom s.r.l.) e di un distinto contratto tra la stessa certification authority e i firmatari ("utilizzatori" del servizio), nonché le banche medesime ("clienti finali")–, le società istanti ritengono, per quanto di rispettiva competenza, di essere autonome titolari dei relativi trattamenti. In particolare, IT Telecom s.r.l. ritiene di essere titolare del trattamento dei dati personali e biometrici dei firmatari ai fini dell'attivazione, erogazione, gestione, amministrazione e manutenzione del servizio mediante i propri sistemi informativi, mentre Cariparma S.p.A. e le altre banche sarebbero autonome titolari dei rispettivi trattamenti "ai fini delle sole operazioni di identificazione, attivazione e successivo utilizzo del servizio", limitatamente alla quota parte di interfacciamento con le proprie piattaforme informative. Ciò, in ragione soprattutto del fatto che le società opererebbero "in modo autonomo nei rispettivi ambiti di competenza" (da considerarsi "nettamente distinti sotto il profilo operativo e organizzativo") e che le banche, comunque, avrebbero un circoscritto potere decisionale in merito alle modalità di esecuzione dell'intero servizio, da rendersi, attraverso IT Telecom s.r.l., in stringente conformità alla normativa vigente in materia di firma digitale.

Per contro, nessun trattamento di dati biometrici sarebbe effettuato da Telecom Italia S.p.A. con riferimento ai dati dei firmatari, operando quest'ultima quale semplice distributore dei servizi erogati da IT Telecom s.r.l.

A sostegno dell'impostazione sostenuta, le società istanti hanno prodotto documentazione relativa, tra l'altro, alla bozza di contratto intercorrente tra Telecom Italia S.p.A. e le banche committenti, nonché copia delle condizioni generali di contratto relative al servizio medesimo.

5. Le valutazioni dell'Autorità.

5.1. 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 dalle parti (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.

Occorre anzitutto rilevare, 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 degli utenti nella fase di autenticazione, alla disciplina del Codice, con particolare riferimento sia alla corretta identificazione del ruolo rivestito da ciascuna delle 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 dalle banche, 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 della certification authority, 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).

5.2. Rispetto al primo profilo, vale in primo luogo evidenziare che la complessa architettura contrattuale prescelta dalle parti per la fornitura e la regolamentazione dell'intero servizio (comprensivo, come detto, delle operazioni di trattamento di dati biometrici a fini di autenticazione) non agevola, di per sé, l'inquadramento della fattispecie sul piano dell'individuazione delle responsabilità relativamente al trattamento dei dati biometrici degli utenti. Ciononostante, pare a questa Autorità che le dichiarazioni rese e la documentazione trasmessa, invero non sempre univocamente rispondenti, abbiano evidenziato elementi tali da far comunque ritenere che la fattispecie in esame, diversamente da quanto sostenuto dalle società istanti, sia più propriamente riconducibile nell'ambito di una contitolarità del medesimo (e unico) trattamento (art. 4, comma 1, lett. f), del Codice); ciò, sia in ragione di quanto di seguito indicato con riferimento a ciascuna delle parti coinvolte, sia alla luce delle 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).

Premesso, infatti, che il servizio di autenticazione biometrica, reso attraverso l'utilizzo in forma "integrata" delle piattaforme informative delle singole banche e di IT Telecom s.r.l., risponde anche e soprattutto all'esigenza –propria tanto degli operatori creditizi e finanziari che della stessa certification authority– di "identificare" in maniera rigorosa e univoca i firmatari (le prime nel rispetto degli obblighi imposti

dalla normativa vigente in materia di antiriciclaggio, la seconda di quelli previsti dalla disciplina in tema di firma digitale)– occorre poi rilevare, con riguardo agli attori a vario titolo coinvolti nella procedura, che dalle dichiarazioni rese dalle parti e dalla documentazione prodotta (della cui genuinità si può essere chiamati a rispondere anche in sede penale ai sensi del già citato art. 168 del Codice), risulta 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. Ciò, a prescindere dal suo riferito ruolo di "contraente principale" (cfr. nota IT Telecom del 21 dicembre 2012, p. 2), desumibile anche dall'allegata bozza di "accordo per la fornitura di servizi relativi alla sottoscrizione e conservazione di documenti informatici";

– le banche:

- determinano le finalità del trattamento (rese note al fornitore e formalizzate anche attraverso la predetta bozza di accordo), richiedendo espressamente, mediante la sottoscrizione di apposito contratto, l'utilizzo del complessivo servizio di firma digitale con autenticazione biometrica fornito concretamente da IT Telecom s.r.l.;
- determinano le modalità di esecuzione del trattamento, limitatamente alle operazioni di raccolta dei dati biometrici degli interessati (cfr. nota IT Telecom s.r.l. del 21 dicembre 2012, p. 3);
- vantano poteri di controllo e verifica, esercitabili a propria discrezione, in merito alle "prestazioni" fornite dalla certification authority (cfr. artt. 5, lett. m), n), o) e p), e 11 della medesima bozza di accordo);
- stabiliscono le modalità alternative di riconoscimento degli utenti in caso di mancata adesione alla procedura di autenticazione biometrica (cfr. "nota integrativa al documento di presentazione", allegata alla nota Cariparma S.p.A. del 27 novembre 2012, p. 6);
- individuano e adottano eventuali ulteriori misure relativamente alla propria infrastruttura informativa (v. nota IT Telecom s.r.l. del 21 dicembre 2012, p. 4);

– IT Telecom s.r.l.:

- determina le finalità del trattamento, rapportandole alla gestione del complessivo servizio di firma digitale offerto alle banche istanti (v. nota IT Telecom del 21 dicembre 2012, p. 2);
- 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 (tra cui il d.lgs. n. 82/2005, recante il "Codice dell'amministrazione digitale");
- individua i soggetti cui eventualmente conferire l'incarico relativamente alle operazioni di identificazione e registrazione dei dati dei firmatari, impartendo loro le relative istruzioni (v. anche l'art. 16 della bozza di contratto del 7 novembre 2012);
- apporta, sulle modalità di erogazione del servizio, le eventuali modifiche richieste dall'evoluzione tecnologica e normativa (cfr. l'art. 3, lett. e), della bozza di contratto del 7 novembre 2012);
- adotta, nell'ambito del complessivo servizio di sottoscrizione con firma digitale (cui il trattamento di dati biometrici è preordinato), tutte le misure necessarie all'organizzazione del medesimo (predisponendo anche la modulistica contenente le condizioni generali di utilizzo del servizio), ivi comprese le misure di sicurezza di cui alla disciplina del Codice (v. l'art. 14 della bozza di contratto del 7 novembre 2012).

Alla luce di tali complessivi elementi, pare dunque difficile, nel caso di specie, ravvisare due distinti trattamenti di dati biometrici in capo alle singole banche e a IT Telecom 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 gli attori coinvolti, ancorché operanti "in sequenza", pongano in essere operazioni differenti di un unico trattamento preordinato all'autenticazione dell'interessato, 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).

5.3. 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. Occorre infatti sottolineare, sul piano generale, che l'identificazione certa e rigorosa dell'utenza, 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 degli utenti in vista della sottoscrizione digitale dei documenti potrebbe, da un lato, contribuire a contrastare efficacemente il crescente numero di frodi dichiarato dalle banche e, dall'altro, snellire e velocizzare (anche a vantaggio della stessa utenza) le operazioni di riconoscimento allo sportello. Deve poi rilevarsi, ancora, che il trattamento in esame, nella misura in cui possa ritenersi effettivamente compatibile con l'attuale quadro normativo applicabile ai servizi di sottoscrizione con firma digitale erogati da IT Telecom s.r.l. (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) può risultare funzionale, ancorché indirettamente, a garantire in concreto l'osservanza degli stringenti obblighi di

riconoscimento degli interessati che la specifica normativa di settore (d.lgs. n. 82/2005, cit.; d.P.C.M. 30 marzo 2009) pone in capo agli stessi enti certificatori ai fini della fornitura del servizio. Considerato, infine, che il trattamento dei dati biometrici dei firmatari, fatto salvo quanto precisato al successivo punto 6, avverrà sulla base del consenso informato degli interessati e per il perseguimento di legittime finalità rese note a questi ultimi, deve ritenersi che, anche alla luce di quanto sopra richiamato, risultino integrati, rispetto alla fattispecie in esame, 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), vale sottolineare 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 sotto il profilo della sicurezza dei dati trattati, si può ritenere che l'immediata cifratura delle informazioni presso le singole banche e la loro trasmissione a IT Telecom s.r.l. per mezzo di canali "https" considerati affidabili, nonché la configurazione di opportune regole di accesso sui firewall previsti presso i data center della certification authority (cfr. documento IT Telecom s.r.l. allegato alla nota del 27 aprile 2012, p. 17), costituiscano misure adeguate ai sensi degli artt. 31 e ss. del Codice. Considerato, poi, che le società hanno anche dichiarato di voler adottare soluzioni organizzative (separazione fisica dei server; ubicazione degli stessi in locali adeguatamente protetti e accessibili dal solo personale autorizzato; tracciamento delle operazioni di accesso ai dati e ai sistemi; ecc.) tali, allo stato, da far ritenere come remoto il rischio di eventuali operazioni indebite sui dati biometrici degli interessati, si può conclusivamente sostenere che il trattamento, per come prospettato, sia conforme, anche in relazione ai profili concernenti le misure di sicurezza, alla disciplina del Codice.

Tanto, sull'ulteriore presupposto che la stessa certification authority –già tenuta ad operare secondo i rigidi standard previsti dalla normativa vigente (d.lgs. n. 82/2005, cit.; d.P.C.M. 30 marzo 2009)– risulta anche soggetta alla stringente vigilanza dell'Agenzia per l'Italia Digitale.

Infine, anche in ragione di quanto previsto dall'art. 11, comma 1, lett. c), del Codice, appare in linea con le disposizioni di legge l'adozione di meccanismi di auto-apprendimento in grado di garantire, nel tempo, la "qualità" dei dati biometrici trattati.

6. Ulteriori adempimenti.

Come anticipato (cfr. punto 2.1), le società provvederanno a rendere agli interessati la prevista informativa nel corso della procedura di adesione al servizio. Tuttavia, nei modelli acquisiti non risultano puntualmente evidenziate le caratteristiche del trattamento relativo ai dati biometrici degli interessati. Le società dovranno pertanto modificare e/o integrare l'informativa da rendere ai firmatari in ordine a tale specifico trattamento, rendendo loro tutti gli elementi di cui all'art. 13 del Codice e soffermandosi, in particolare, sulla tipologia di dati raccolti e sulle informazioni da essi desumibili, sul profilo della co-titolarità (art. 13, comma 1, lett. f), del Codice) e sulle finalità distintamente perseguite da ciascun co-titolare nell'ambito della procedura di autenticazione biometrica (art. 13, comma 1, lett. a), del Codice).

Inoltre, fatta salva l'eventuale applicabilità di specifiche normative e l'esigenza di ulteriore conservazione derivante da eventuali contestazioni in sede anche giudiziaria, i dati biometrici degli interessati dovranno essere conservati dalle parti per il periodo di tempo strettamente necessario al perseguimento degli scopi per i quali gli stessi sono stati raccolti e successivamente trattati (art. 11, comma 1, lett. e), del Codice) e cancellati immediatamente, ovvero nei tempi tecnici a tal fine necessari e, comunque, non oltre l'indicato termine di 30 giorni.
Infine, le società dovranno provvedere, prima dell'inizio del trattamento, a modificare la notifica già effettuata in conformità agli artt. 37 e ss. del Codice.

Resta inteso, ovviamente, che il trattamento dei dati biometrici degli interessati potrà considerarsi lecito, nel caso di specie, solo ove il loro consenso venga realmente acquisito in forma effettivamente libera (art. 23 del Codice), non potendo considerarsi tale quello raccolto in conseguenza di eventuali pressioni o condizionamenti anche in occasione dell'adesione al servizio (in proposito, cfr., da ultimo, Provv. 4 ottobre 2012, doc. web n. 2059743). 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 riferita possibilità, da parte di ciascuna banca, di assicurare comunque la fruizione del servizio di sottoscrizione dei documenti con firma digitale attraverso modalità alternative di autenticazione.

TUTTO CIÒ PREMESSO, IL GARANTE,

ai sensi dell'art. 17 del Codice, a conclusione della verifica preliminare richiesta da Cassa di Risparmio di Parma e Piacenza S.p.A., Banca Popolare Friuladria S.p.A., Cassa di Risparmio della Spezia S.p.A. e IT Telecom 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, ammette il trattamento dei dati biometrici nei termini di cui in narrativa e nel doveroso rispetto di quanto dichiarato dagli istanti ai sensi dell'art. 168 del Codice, e a condizione che le società provvedano a:

1. modificare e/o integrare l'informativa da rendere agli interessati, indicando puntualmente tutti gli elementi di cui all'art. 13 del Codice e soffermandosi, in particolare, sui profili relativi alla tipologia di dati raccolti e le informazioni da essi desumibili, alla co-titolarità e alle finalità del trattamento;

2. acquisire un consenso realmente libero da parte degli interessati, in aderenza a quanto disposto dall'art. 23 del Codice;

3. conservare i dati biometrici degli interessati, fatte salve l'eventuale applicabilità di normative specifiche e le esigenze di ulteriore conservazione derivanti da eventuali contestazioni in sede anche giudiziaria, per il periodo di tempo strettamente necessario al perseguimento degli scopi per cui gli stessi sono stati raccolti e successivamente trattati (art. 11, comma 1, lett. e) del Codice), provvedendo altresì alla loro immediata cancellazione, ovvero nei tempi tecnici a tal fine necessari e,

comunque, non oltre l'indicato termine di 30 giorni;

4. modificare, antecedentemente all'inizio del trattamento medesimo, le notifiche già effettuate in conformità agli artt. 37 e ss. 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