Installazione di un sistema completamente automatizzato di cassette di sicurezza. Verifica preliminare richiesta da Cassa Raiffeisen di Lagundo Soc. coop - 13 settembre 2012

Registro dei provvedimenti

n. 242 del 13 settembre 2012

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

Esaminata la richiesta di verifica preliminare presentata dalla Cassa Raiffeisen di Lagundo Soc. coop. ai sensi dell'art. 17 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), relativa all'installazione di un sistema di rilevamento biometrico per l'accesso della clientela alle cassette di sicurezza;

Visti gli atti d'ufficio;

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

Relatore la dott.ssa Giovanna Bianchi Clerici;

PREMESSO

1. L'istanza della Banca e le modalità di funzionamento del sistema.

1.1. In data 28 novembre 2011, la Cassa Raiffeisen di Lagundo Soc. coop. ha presentato una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, in vista dell'installazione di un sistema "completamente automatizzato di cassette di sicurezza, denominato "Safestore Auto Maxi", […], volto a consentire a ciascun cliente […di] accedere alla sua cassetta di sicurezza 365 giorni all'anno, nell'arco delle 24 ore e senza l'intervento del […] personale [della Banca]" (cfr. comunicazione della Raiffeisen del 19 ottobre 2010, p. 1).

Secondo quanto riferito, il sistema in questione sarebbe innovativo in quanto, consentendo la sicura identificazione dei clienti mediante una rilevazione dell'impronta digitale, da un lato permetterebbe alla Banca di garantire la custodia dei beni depositati nelle cassette di sicurezza, dall'altro porrebbe la clientela in condizione di usufruire di tale servizio anche al di fuori dell'orario di sportello della Banca.

Per quanto concerne il funzionamento del sistema, ai clienti che intendessero utilizzare il dispositivo di cassette self service verrebbe fornita una smart card –che resterebbe nella esclusiva disponibilità di costoro– contenente un microchip nel quale sarebbe memorizzato un codice numerico (template) convertito dall'impronta digitale del cliente; quindi, "una volta ultimata la procedura di registrazione, l'impronta digitale del cliente non [sarebbe] più accessibile alla Banca", visto che non [verrebbe] memorizzata" e tenuto conto che " i dati si [troverebbero] esclusivamente sulla tessera consegnata al cliente", la quale sarebbe priva di ulteriori informazioni personali.

Al momento dell'accesso al servizio relativo alle cassette di sicurezza, "l'autenticazione del cliente" avverrebbe "attraverso tre strumenti: codice PIN di quattro cifre, smart card e impronta digitale". In particolare, il sistema prevede che il cliente inserisca la propria smart card, digiti il PIN e proceda al rilevamento della propria impronta biometrica, che successivamente verrebbe confrontata con il template memorizzato nella smart card.

Per i clienti che non intendessero avvalersi del sistema, sarebbero comunque previste modalità alternative per usufruire del servizio concernente le cassette di sicurezza, basate soltanto sull'utilizzazione della smart card e del PIN. In tal caso, però, il servizio sarebbe fruibile solo durante "l'orario di sportello e previa identificazione personale da parte degli operatori della Banca" (cfr. comunicazione della Banca del 22 novembre 2011).

Inoltre, è prevista anche l'installazione di un impianto di videosorveglianza in prossimità del locale al quale si dovrebbe accedere per usufruire del servizio relativo alle cassette di sicurezza, che registrerebbe alcuni fotogrammi che verrebbero salvati nel database interno al dispositivo ed automaticamente cancellati dopo sette giorni. Ad essi verrebbe "associato il nominativo del cliente che ha effettuato l'accesso al dispositivo e l'orario dell'operazione" (cfr. doc. Gunnebo p. 2, allegato alla nota del 19 ottobre 2010).

Infine, è stabilito che l'accesso al Sistema Safestore Auto (che, comunque, non conterrà i dati biometrici dei clienti) sarà consentito solo al personale incaricato provvisto di apposita password (costituita da un codice numerico di riconoscimento a 8 cifre), la quale avrà un periodo di validità non superiore a 150 giorni, allo scadere del quale il codice dovrà essere aggiornato. Inoltre, ai dipendenti incaricati di accedere alla zona delle cassette di sicurezza, verrà rilasciata un'apposita tessera denominata Mastercard.

2. I presupposti di liceità del trattamento.

La raccolta e la registrazione di impronte digitali e dei dati biometrici, ricavati e successivamente utilizzati per verifiche e raffronti nelle procedure di autenticazione o di identificazione, sono operazioni di trattamento di dati personali riconducibili ai singoli interessati (art. 4, comma 1, lett. b) del Codice), rispetto alle quali trova applicazione la normativa contenuta nel Codice (in merito v. anche i documenti di lavoro sulla biometria del "Gruppo art. 29" della direttiva 95/46/Ce: Wp 80 del 1° agosto 2003 e WP 193 del 27 aprile 2012).

Pertanto, la liceità del sistema in questione deve essere valutata alla luce dei principi di necessità, proporzionalità, finalità e correttezza del trattamento (artt. 3 e 11 del Codice), considerando, in particolare, il contesto in cui tali dati sono trattati.

Nel caso di specie, si rileva che la finalità perseguita dalla Banca (che assume la veste di titolare del trattamento) è quella di coniugare l'esigenza di tutela dei beni custoditi nelle cassette di sicurezza con l'utilità garantire alla clientela un servizio continuato di custodia, attraverso l'implementazione di un sistema che, "per le modalità con le quali è configurato", possa "scongiurare l'accesso fraudolento alle cassette di sicurezza" (in tal senso, v. anche Provv. 15 aprile 2010, doc. web n. 1719879). Tale finalità risulta lecita.

Inoltre, il trattamento posto in essere dalla Banca può anche considerarsi proporzionato, in quanto, nel caso specifico, non è prevista una conservazione dei dati biometrici raccolti in archivi centralizzati, ma il dato criptato dell'impronta digitale verrà memorizzato esclusivamente sulla smart card, che resterà nell'esclusiva disponibilità del cliente che avrà aderito al servizio. Tale modalità di memorizzazione risulta idonea a garantire un adeguato livello di accuratezza in ordine all'accertamento dell'identità del detentore della smart card e, nello stesso tempo, ad evitare il rischio di eventuali utilizzi impropri o possibili abusi che, invece, potrebbero derivare dalla raccolta di tali informazioni, particolarmente delicate, in un sistema centralizzato.

3. Ulteriori adempimenti.

In relazione all'informativa, si prende atto che la Banca, assumendo ogni responsabilità al riguardo (art. 168 del Codice), ha dichiarato che i soggetti interessati all'utilizzo del sistema riceveranno un'informativa scritta, distinta da quella generale, rispetto al trattamento di dati personali e biometrici (cfr. punto 20 della nota del 22 novembre 2011).

Ciò premesso, si deve richiamare l'attenzione della Banca sul fatto che la medesima informativa dovrà indicare chiaramente anche la possibilità per gli interessati –che non vogliano o non possano, anche in ragione di proprie caratteristiche fisiche, servirsi del sistema di riconoscimento biometrico– di utilizzare modalità alternative (già individuate dalla Banca) per avvalersi comunque del servizio relativo alle cassette di sicurezza.

E' evidente, poi, che l'utilizzo dei dati biometrici, per risultare lecito, non potrà prescindere dal previo rilascio di un apposito consenso da parte degli interessati (art. 23 del Codice).

Riguardo alle misure di sicurezza, esse risultano adeguate, anche per quanto concerne gli accorgimenti che, al fine di prevenire accessi indebiti, saranno tenuti ad osservare i dipendenti che gestiranno il Sistema "Safestore Auto Maxi" (nome utente e password), e quelli che dovranno accedere, nello svolgimento della propria attività lavorativa, all'area delle cassette di sicurezza (tessera Mastercard). In attuazione dell'obbligo di adottare ogni necessaria misura di sicurezza, anche minima (art. 31 ss. e all. B) al Codice), la Banca dovrà comunque anche conservare una descrizione scritta dell'intervento effettuato dall'installatore,

che attesti anche la conformità del Sistema alle disposizioni del disciplinare tecnico (regola n. 25 dell'all. B) al Codice).

Infine, resta inteso che la Banca non solo dovrà procedere alla designazione per iscritto degli incaricati del trattamento, impartendo loro idonee istruzioni alle quali attenersi (artt. 4, comma 1, lett. h) e 30 del Codice), ma dovrà altresì effettuare la notifica obbligatoria al Garante, prima che abbiano inizio le operazioni di trattamento dei dati biometrici (art. 37, comma 1, lett. a) del Codice).

TUTTO CIÒ PREMESSO IL GARANTE

a conclusione della verifica preliminare relativa al sistema "Safestore Auto Maxi" che la Cassa Raiffeisen di Lagundo Soc. coop. intende installare per consentire, senza l'intervento del personale, l'accesso continuato dei propri clienti al servizio relativo alle cassette di sicurezza, prende atto del trattamento oggetto delle dichiarazioni rese e della documentazione prodotta, fermo restando, quali prescrizioni ai sensi degli artt. 17 e 154, comma 1, lett. c) del Codice, che la Banca dovrà:

1. indicare chiaramente nell'informativa la possibilità per gli interessati di avvalersi del servizio relativo alle cassette di sicurezza con modalità alternative rispetto alla rilevazione dei loro dati biometrici;

2. conservare una descrizione scritta dell'intervento effettuato dall'installatore, che attesti anche la conformità del Sistema alle disposizioni del disciplinare tecnico (regola n. 25 dell'all. B al Codice);

3. designare per iscritto gli incaricati del trattamento, impartendo loro idonee istruzioni alle quali attenersi (artt. 4, comma 1, lett. h) e 30 del Codice);

4. notificare al Garante il trattamento dei dati biometrici prima che abbiano inizio le operazioni di trattamento (art. 37, comma 1, lett. a) del Codice).

Roma, 13 settembre 2012

IL PRESIDENTE

Soro

IL RELATORE

Bianchi Clerici

IL SEGRETARIO GENERALE

Busia