[doc. web n. 2375735]

Sistema per l'accesso della clientela in modalità c.d. self service, 24 ore su 24 alle cassette di sicurezza che può prevedere il trattamento di dati biometrici. Verifica preliminare richiesta da Banca di credito cooperativo di Vigevano - 14 febbraio 2013

Registro dei provvedimenti
n. 66 del 14 febbraio 2013

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro 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 Banca di Credito Cooperativo di Vigevano s.c., ai sensi dell'art. 17 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), relativa all'attivazione di un sistema biometrico per l'accesso dei clienti alla propria cassetta 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.

1.1. In data 27 giugno 2012, la Banca di Credito Cooperativo di Vigevano s.c. (di seguito, "Banca") ha presentato una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice per l'attivazione, "presso la […] filiale di via Trivulzio 23 a Vigevano (PV) di prossima apertura", di un sistema per l'accesso della clientela −in modalità c.d. self service, 24 ore su 24− alle cassette di sicurezza, "che può prevedere il trattamento di dati biometrici". Tale forma di accesso avverrebbe solo su base volontaria, ferma restando la possibilità -per i clienti che non intendessero avvalersi di questo sistema- di accedere al locale delle cassette di sicurezza attraverso modalità tradizionali, con l'utilizzo di una smart card abbinata ad un PIN.

Secondo quanto riferito dalla Banca, l'installazione del sistema −che riguarderebbe settantuno cassette− avrebbe lo scopo di aumentare la sicurezza dei clienti, che potrebbero "accedere alle cassette di sicurezza al di fuori degli orari di sportello con piena garanzia della propria incolumità" e con "l'assoluta certezza" dell'inviolabilità delle stesse da parte di terzi (v. citata comunicazione del 27 giugno 2012, p. 2 e 3).

1.2. Le modalità di funzionamento del sistema

Come già detto, a ciascun cliente che intendesse usufruire del servizio relativo alle cassette di sicurezza la Banca offrirebbe due distinte modalità di accesso: quella con il sistema biometrico oppure quella con modalità tradizionali (smart card e PIN). Se il cliente dovesse optare per il sistema biometrico, la Banca gli fornirebbe una specifica informativa sul trattamento dei dati personali e biometrici, acquisendo anche il suo consenso; successivamente, il cliente verrebbe invitato a rilasciare l'impronta digitale, appoggiando il dito su un apposito lettore che genererebbe "un algoritmo matematico univoco ed irripetibile", il quale verrebbe "memorizzato su una smart card". Quindi, la Banca consegnerebbe al cliente la smart card e il relativo PIN (codice numerico di accesso), che sarebbe definito dallo stesso cliente al momento della prima registrazione e, poi, modificato fin dal primo accesso.

Al momento dell'accesso al locale riservato alle cassette di sicurezza, il cliente prima inserirebbe la smart card nel lettore deputato a consentire l'apertura della porta, poi in quello destinato al riconoscimento dell'utente; quindi, il cliente digiterebbe il PIN e appoggerebbe il proprio dito sull'apposito scanner, permettendo al sistema di verificare la corrispondenza tra l'algoritmo matematico generato dall'impronta digitale e quello memorizzato sulla smart card. In caso di verifica positiva, la cassetta di sicurezza assegnata al cliente sarebbe prelevata dalla cassaforte attraverso un sistema elettro-meccanico.

Nella fase di riconoscimento, una webcam integrata rileverebbe dieci fotogrammi del volto del cliente, che sarebbero "associati esclusivamente all'anagrafica del cliente" (v. comunicazione della Banca del 22 gennaio 2013) e conservati nel sistema per sette giorni, al termine dei quali le immagini verrebbero cancellate automaticamente.

Nel locale self service non verrebbero collocati sistemi di videosorveglianza, né effettuate videoriprese (v. cit. comunicazione del 27 giugno 2012, p. 5).

1.3 Le misure di sicurezza

La Banca ha dichiarato che, al fine di prevenire "possibili pregiudizi ai danni dei clienti interessati", con particolare riguardo a condotte illecite volte alla "abusiva ricostruzione dell'impronta digitale", sarebbe "esclusa qualsiasi forma di memorizzazione in archivi situati presso la banca dei dati biometrici in questione". Infatti, il sistema si baserebbe sulla lettura di impronte digitali acquisite nella forma di template cifrati, successivamente memorizzati su smart card prive di indicazioni nominative dei clienti e poste nella loro esclusiva disponibilità. I dati biometrici sarebbero trattati "esclusivamente durante la fase di realizzazione del template" e coloro che fossero chiamati alla loro registrazione sulle smart card verrebbero nominati "incaricati del trattamento", così come i dipendenti che dovessero svolgere attività di manutenzione sul sistema (denominato "Safestore Auto").

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, finalità, proporzionalità, 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 – in qualità di titolare del trattamento− è quella di "aumentare la sicurezza della clientela durante l'accesso in modalità self-service alle cassette di sicurezza, che possono contenere documenti riservati, oggetti di valore o denaro e quindi possono rappresentare un concreto obiettivo di furti e rapine", consentendo, nello stesso tempo, l'accesso anche "al di fuori degli orari di sportello con piena garanzia della propria incolumità" (in tal senso, v. anche Provv.ti 15 aprile 2010, doc. web n. 1719879; 13 settembre 2012, doc. web n. 1927441). 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. Ciò risulta altresì conforme al principio di necessità (art. 3 del Codice), secondo il quale i sistemi informativi devono essere configurati in modo da ridurre al minimo l'utilizzazione di dati personali, escludendone il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate con altre modalità (in particolare, mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità).

3. Ulteriori adempimenti.

In relazione all'informativa, si prende atto che la Banca ha dichiarato che i soggetti interessati all'utilizzo del sistema riceveranno, prima di procedere alla raccolta del dato biometrico, una specifica informativa scritta sul trattamento dei loro dati personali e biometrici, diversa e distinta da quella che verrà fornita a coloro che decideranno di utilizzare le modalità tradizionali di accesso ai locali della cassette di sicurezza; inoltre, si prende altresì atto che dagli interessati verrà acquisito il consenso previsto dall'art. 23 del Codice (v. cit. comunicazione Banca, p. 4 e 5).

Ciò premesso, si richiama 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 o che successivamente decidano di non avvalersene più– di utilizzare modalità alternative (già individuate dalla Banca) per avvalersi comunque del servizio relativo alle cassette di sicurezza.

Riguardo alle misure di sicurezza, risulta adeguata la scelta di memorizzare il dato biometrico –in forma di template- esclusivamente su una smart card prodotta in un unico esemplare, posta nella sola disponibilità del cliente e priva di suoi riferimenti nominativi.

Si prende altresì atto che la Banca designerà quali incaricati del trattamento i dipendenti che effettueranno le operazioni di trattamento dei dati biometrici attraverso la registrazione del template sulla smart card, impartendo loro idonee istruzioni alle quali attenersi, nonché i dipendenti che svolgeranno l'attività di manutenzione sul sistema "Safestore Auto"; a tale proposito, la Banca, con nota del 22 gennaio 2013, ha specificato che "per ogni incaricato/categoria omogenea di incaricati del trattamento" verrà "definito uno specifico profilo di autorizzazione coerente con le attività svolte".

Resta inteso che la Banca, oltre a procedere alle suddette designazioni, in attuazione dell'obbligo di adottare ogni necessaria misura di sicurezza, anche minima (art. 31 ss. e all. B) al Codice), dovrà comunque 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); inoltre, la stessa 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 Banca di credito cooperativo di Vigevano 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 -della cui veridicità gli istanti rispondono penalmente ai sensi dell'art. 168 del Codice- 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. designare per iscritto gli incaricati del trattamento, impartendo loro idonee istruzioni alle quali attenersi (artt. 4, comma 1, lett. h) e 30 del Codice);

3. 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);

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, 14 febbraio 2013

IL PRESIDENTE
Soro

IL RELATORE
Bianchi Clerici

IL SEGRETARIO GENERALE
Busia