



**Sistema di videosorveglianza. Verifica preliminare richiesta da Banca d'Italia - 22 maggio 2014**

Registro dei provvedimenti  
n. 259 del 22 maggio 2014

**IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, 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.lgs. 30 giugno 2003, n. 196);

VISTO il provvedimento generale in materia di videosorveglianza adottato dal Garante l'8 aprile 2010;

ESAMINATA la richiesta di verifica preliminare presentata dalla Banca d'Italia ai sensi dell'art. 17 del Codice, riguardante l'installazione di sistemi di videosorveglianza presso la sede dell'Amministrazione centrale e delle filiali (nota del 19 novembre 2013, Prot. n. 1070926/13; nota del 25 marzo 2014, Prot. n. 0324911/14);

VISTA la documentazione in atti;

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

RELATORE la dott.ssa Augusta Iannini;

**PREMESSO**

La Banca d'Italia ha presentato a questa Autorità una richiesta di verifica preliminare, ai sensi dell'art. 17 del Codice, con riferimento al trattamento di dati personali che intende effettuare mediante sistemi di videosorveglianza intelligenti da installare presso le sedi dell'Amministrazione centrale e delle filiali, al fine di "garantire la sicurezza degli edifici e dei beni".

Secondo la Banca d'Italia, i sistemi di videosorveglianza intelligenti in esame sono volti "ad assicurare una maggiore efficacia delle misure di sicurezza anticrimine, in relazione agli specifici rischi connessi con le attività svolte nei siti interessati (trattamento e stoccaggio di elevate quantità di valori)".

In particolare, il trattamento di dati personali sottoposto alla verifica preliminare riguarda l'utilizzo di sistemi di videosorveglianza che prevedono l'attivazione "in chiave di prevenzione di atti criminosi e controllo accessi" di talune "funzioni speciali", di seguito indicate:

- "lettura targhe e identificazione mezzi";
- "motion detection digitale";
- "controllo ambientale", nelle fattispecie relative al "riconoscimento oggetto abbandonato", "riconoscimento mancanza oggetto", "barriera allarme virtuale", "zona di allarme virtuale", "conteggio", "riconoscimento presenza persone";
- "automazione accesso su chiamata citofonica".

Più precisamente, la Banca d'Italia, nel descrivere i sistemi di videosorveglianza in questione, ha dichiarato che:

- il sistema di videosorveglianza che si intende realizzare è "pienamente conforme alle disposizioni della legge n. 300 del 20 marzo 1970 ("Statuto dei lavoratori") poiché lo stesso non ha alcuna finalità di controllo a distanza dell'attività dei lavoratori essendo interamente ed esclusivamente dedicato a garantire la sicurezza degli edifici e dei beni dell'Istituto";

- le "cosiddette "funzioni speciali" (...) sono attivabili dagli addetti al Posto di controllo per un sottoinsieme di telecamere dedicate alla rilevazione di intrusioni in zone specifiche dello stabile e non sono utilizzate per l'analisi di comportamenti anomali all'interno dei locali della Banca";

- "gli incaricati delle attività di controllo di ciascuno degli edifici interessati possono visionare per finalità di identificazione a distanza e di controllo-tipicamente per individuare la possibile causa di una segnalazione di allarme prodotta dagli impianti di sicurezza- le immagini riprese in tempo reale da tutte le telecamere, richiamandole, all'occorrenza, su monitor dedicati";

- la funzione di controllo ambientale "consente la generazione di eventi di allarme a fronte dell'analisi della scena ripresa e la relativa visualizzazione degli stessi sulle postazioni degli addetti";

- "il periodo di mantenimento delle immagini registrate è di 7 gg., a ricoprimento automatico tramite le funzioni rese disponibili dalla specifica piattaforma software che ne gestisce l'archiviazione".

## OSSERVA

### 1. Verifica preliminare e caratteristiche tecniche del sistema di videosorveglianza.

La richiesta di verifica preliminare sottoposta a questa Autorità riguarda un trattamento di dati personali che la Banca d'Italia intende effettuare attraverso peculiari sistemi di videosorveglianza.

In generale, il trattamento di dati personali mediante l'utilizzo di sistemi di videosorveglianza può essere svolto nel rispetto delle disposizioni contenute nel Codice e delle indicazioni fornite dal Garante nel provvedimento generale in materia di videosorveglianza dell'8 aprile 2010 (consultabile sul sito [www.garanteprivacy.it](http://www.garanteprivacy.it), doc. web n. [1712680](#), pubblicato in G.U. n. 99 del 29 aprile 2010).

Il titolare è tenuto a richiedere una verifica preliminare a questa Autorità nei soli casi in cui i trattamenti che intende effettuare tramite sistemi di videosorveglianza comportino rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare (art. 17 del Codice).

Al riguardo, il citato provvedimento del 2010 prevede che l'obbligo di richiedere la verifica preliminare al Garante sussiste, in particolare, con riferimento ai sistemi di videosorveglianza c.d. intelligenti, che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli e, eventualmente, registrarli. In tali ipotesi, l'Autorità ha stabilito che l'utilizzo dei predetti sistemi risulta giustificato solo in casi particolari, tenendo conto delle finalità e del contesto in cui essi sono trattati, da verificare caso per caso sul piano della conformità ai principi di necessità, proporzionalità, finalità e correttezza (cfr. punto 3.2.1. del citato provvedimento generale).

In tale quadro, i sistemi di videosorveglianza che la Banca d'Italia ha inteso sottoporre alla verifica preliminare dell'Autorità sono abilitati a svolgere talune funzioni speciali, di seguito indicate:

1. "lettura targhe e identificazione mezzi";
2. "motion detection digitale";
3. "controllo ambientale", riconducibile a:
  - a) "riconoscimento oggetto abbandonato";
  - b) "riconoscimento mancanza oggetto";
  - c) "barriera allarme virtuale";
  - d) "zona di allarme virtuale";
  - e) "conteggio";
  - f) "riconoscimento presenza persone";
4. "automazione accesso su chiamata citofonica".

Al riguardo, si ritiene che tra le funzioni descritte soltanto quelle di "controllo ambientale" connesse alla generazione di eventi d'allarme a fronte del superamento di una "barriera allarme virtuale", dell'accesso ad una "zona di allarme virtuale", nonché del "riconoscimento presenza persone" (punto 3, lett. c), d) e f)) risultino idonee a rilevare automaticamente, segnalare e registrare comportamenti o eventi anomali, quali possono considerarsi gli accessi nelle zone interdette anche in relazione a determinate fasce orarie.

In tale quadro, pertanto, risulta correttamente sottoposto alla verifica preliminare dell'Autorità (cfr. punto 3.2.1. del predetto provvedimento generale) soltanto il trattamento dei dati personali che si intende effettuare attraverso sistemi di videosorveglianza, attivando la predetta funzione di controllo ambientale, limitatamente alla "barriera allarme virtuale", "zona di allarme virtuale" e "riconoscimento presenza persone" (punto 3, lett. c), d) e f)).

Le ipotesi residue descritte ("lettura targhe e identificazione mezzi", "motion detection digitale", "automazione accesso su chiamata citofonica", "conteggio", "riconoscimento oggetto abbandonato" e "mancanza oggetto") non rientrano, invece, tra le ipotesi previste dal

provvedimento generale in cui è necessario sottoporre i sistemi di videosorveglianza alla verifica preliminare dell'Autorità. Ciò in quanto, in relazione alle funzioni di "lettura targhe e identificazione mezzi", "motion detection digitale", "automazione accesso su chiamata citofonica" e "conteggio" (punti 1, 2, 3, lett. e) e 4) non è prevista la generazione di allarmi; in relazione alle funzioni di "riconoscimento oggetto abbandonato" e "mancanza oggetto" (punto 3, lett. a), e b)), che prevedono, rispettivamente, l'attivazione di un allarme se un oggetto viene abbandonato all'interno dell'inquadratura di una o più telecamere "per un certo periodo di tempo" e se un oggetto esistente viene rimosso dall'inquadratura, non riguardando persone, non comportano un trattamento di dati personali.

## **2. Presupposti di liceità e proporzionalità del trattamento di dati personali in esame.**

La Banca d'Italia, in qualità di titolare del trattamento, può trattare dati personali nel rispetto del principio di finalità, perseguendo scopi determinati, espliciti e legittimi, per lo svolgimento delle proprie funzioni istituzionali (cfr. artt. 4, comma 1, lett. f); 11, comma 1, lett. b); 18, comma 2, del Codice; punto 5 del citato provvedimento generale).

Alla luce degli specifici compiti assegnati alla Banca d'Italia, con particolare riferimento all'emissione delle banconote in euro e al servizio di Tesoreria provinciale e centrale dello Stato, in base al quale la medesima Banca d'Italia esegue le disposizioni di pagamento emesse dalle amministrazioni dello Stato, riscuote le somme dovute a qualsiasi titolo allo Stato, sia direttamente sia indirettamente attraverso le banche, le Poste e i concessionari della riscossione e riceve e custodisce depositi in buoni postali e contante, la Banca d'Italia persegue legittime finalità di sicurezza degli edifici e dei beni, anche attraverso l'installazione di sistemi di videosorveglianza.

Tenuto conto che la stessa Banca d'Italia ha espressamente evidenziato che i sistemi di videosorveglianza in esame non sono in alcun modo finalizzati ad un controllo dell'attività dei lavoratori, si rileva che, in ogni caso, qualora tale attività di videosorveglianza possa realizzare, pur non essendovi preordinata, un controllo a distanza dell'attività lavorativa, resta ferma l'esigenza che venga rispettato il provvedimento generale del Garante dell'8 aprile 2010, con particolare riferimento alle garanzie previste al riguardo per i lavoratori (punto 4.1.; art. 114 del Codice; art. 4, legge 20 maggio 1970, n. 300).

In tale quadro, si ritiene che i sistemi di videosorveglianza correttamente sottoposti alla verifica preliminare dell'Autorità (riconducibili alle funzioni di "barriera allarme virtuale", "zona di allarme virtuale", "riconoscimento della presenza di persone" (cfr. punto 3, lett. c), d) e f)), sulla base degli elementi acquisiti in atti e valutata la proporzionalità del trattamento dei dati personali effettuati mediante gli stessi, non comportino, in concreto, un pregiudizio rilevante per gli interessati, idoneo a determinare effetti particolarmente invasivi sulla loro sfera di autodeterminazione e, conseguentemente, sui loro comportamenti. Le caratteristiche specifiche dei sistemi in esame, infatti, nel rilevare il superamento di una barriera virtuale, delimitata da una linea predefinita, e l'accesso ad una zona interdotta segnalata con la "presenza di idonei cartelli informativi e (con) dispositivi di delimitazione delle zone protette", nonché il procedere nel senso sbagliato in un percorso predefinito, producono l'effetto esclusivo di richiamare l'attenzione degli addetti al posto di controllo, al fine di favorire un eventuale tempestivo intervento, volto a verificare la fondatezza della segnalazione d'allarme.

Dalla documentazione trasmessa in atti, risulta che tali sistemi di videosorveglianza prevedono funzioni con "finalità antintrusione e di supporto alla safety, attivabili sulle telecamere che riprendono gli accessi e alcune zone interne dello stabile particolarmente sensibili ai fini della sicurezza" (es. zona dei caveaux), e non attivano ulteriori funzionalità, anche eventualmente legate al comportamento dell'interessato ripreso, quali, ad esempio, l'analisi audio, la geolocalizzazione o il riconoscimento tramite incrocio con ulteriori specifici dati personali, anche biometrici, o confronto con una campionatura preconstituita.

Ciò premesso, allo stato degli elementi acquisiti e della documentazione esaminata, valutate le rappresentate esigenze di sicurezza dei predetti edifici (sede dell'Amministrazione centrale e delle filiali), connesse anche alle specifiche funzioni di tesoreria e di emissione di banconote svolte dalla Banca d'Italia, si ritiene proporzionato e, quindi, ammissibile il trattamento dei dati personali che la stessa intende effettuare per le predette finalità di sicurezza tramite i sistemi di videosorveglianza riconducibili alle funzioni di "barriera allarme virtuale", "zona di allarme virtuale", "riconoscimento della presenza di persone" (cfr. punto 3, lett. c), d) e f) nei termini e con le modalità sopra evidenziate.

In ogni caso, nell'ambito degli adempimenti previsti dal Codice e dal citato provvedimento generale, in relazione al trattamento di dati personali effettuato, in generale, mediante sistemi di videosorveglianza, si richiama l'attenzione della Banca d'Italia sulle:

- prescrizioni relative alle misure minime di sicurezza, con particolare riferimento all'obbligo di adottare specifici accorgimenti tecnici ed organizzativi che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (cfr. punto 3.3.1. del citato provvedimento generale; artt. 31-36 del Codice e allegato B al Codice);
- indicazioni in materia di informativa gli interessati (cfr. punto 3.1. del citato provvedimento generale; art. 13 del Codice);
- garanzie previste in materia di controllo a distanza dell'attività lavorativa (cfr. punto 4.1. del citato provvedimento generale; art. 114 del Codice; art. 4, legge 20 maggio 1970, n. 300).

### **TUTTO CIÒ PREMESSO IL GARANTE**

ai sensi dell'art. 17 del Codice, accoglie, nei termini e con le modalità sopra descritte, la richiesta di verifica preliminare presentata dalla Banca d'Italia in relazione al trattamento di dati personali che intende effettuare per finalità di sicurezza tramite i predetti sistemi di videosorveglianza da installarsi presso le sedi dell'Amministrazione centrale e delle filiali.

Roma, 22 maggio 2014

IL PRESIDENTE

Soro

IL RELATORE  
Iannini

IL SEGRETARIO GENERALE  
Busia