



Sistema di videosorveglianza installato presso un esercizio commerciale - 17 gennaio 2013

Registro dei provvedimenti
n. 16 del 17 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, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

ESAMINATA la documentazione in atti;

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

VISTO il provvedimento generale del Garante dell'8 aprile 2010, in materia di trattamento di dati personali effettuato tramite sistemi di videosorveglianza (G.U. n. 99 del 29 aprile 2010 e in www.garanteprivacy.it, doc. web n. [1712680](#));

VISTI il verbale di accertamento ispettivo del 4 agosto 2011, integrato dal verbale del 3 ottobre 2011 (corredato da riprese fotografiche), entrambi trasmessi al Garante con nota del 6 ottobre 2011 dalla Questura di Genova - Divisione Polizia amministrativa, aventi ad oggetto un impianto di videosorveglianza funzionante presso l'esercizio commerciale FNAC di Genova (di seguito, la società), dai quali emerge che:

- il menzionato sistema di videosorveglianza, è composto di 30 telecamere (14 delle quali brandeggiabili), dislocate nell'area di vendita, in parte del perimetro esterno, in corrispondenza delle aree deputate allo scarico merci e alla cassa continua, nonché in corrispondenza dell'accesso riservato a dipendenti e fornitori – ove pure è collocato il dispositivo di rilevazione delle presenze dei dipendenti –, nel magazzino merci nonché in prossimità dell'ingresso alle toilette riservate sia al personale che alla clientela (cfr. verbale 4 agosto 2011);
- le telecamere, in parte fisse e in parte mobili, sono "a colori, ad alta risoluzione"; alcune di esse sono in grado di effettuare ingrandimenti;
- un accordo con le rappresentanze sindacali del 27 febbraio 2001 stipulato ai sensi dell'art. 4, comma 2, l. 20 maggio 1970, n. 300 ne regola il funzionamento e nello stesso (acquisito agli atti) si chiarisce che:
 - gli apparati di ripresa sono stati installati "con funzione anti-rapina e anti-taccheggio", con esclusione del possibile utilizzo dello stesso "ai fini disciplinari";
 - le immagini memorizzate sono custodite in un apposito armadio di sicurezza con accesso a doppia chiave, poste l'una nella disponibilità del responsabile della sicurezza del negozio, l'altra di un rappresentante sindacale aziendale;
- le immagini riprese mediante il sistema di videosorveglianza sono visualizzate (e registrate per 24 ore) presso l'esercizio commerciale in una sala controllo dove opera un dipendente di altra società (IS Roma Sicurezza) le cui mansioni sono risultate, tra le altre, quelle di verifica del "flusso della clientela in entrata e in uscita; [questi] inoltre controlla attraverso i monitor eventuali tentativi di sottrazione di merce. Nel caso in cui rilevi un soggetto autore di furto, avverte il responsabile del punto vendita [che attende] la persona oltre la barriera delle casse e la invita a seguirlo in un ufficio adiacente alla barriera " (cfr. dichiarazioni rese nel verbale del 4 agosto 2011);
- il responsabile della sicurezza e del trattamento dei dati presso l'esercizio commerciale ha confermato che gli incaricati di IS Roma Sicurezza, tra l'altro, "collaborano nella gestione dei flussi di persone all'interno del punto vendita; nel caso in cui notino comportamenti che possano arrecare danno all'azienda avvertono il responsabile del negozio" (cfr. verbale 3 ottobre 2011);
- tale sistema di sorveglianza risulta integrato "presso l'ufficio del coordinatore di IS Roma Sicurezza [da] una posizione remota che permette di vedere le immagini in tempo reale" (cfr. verbale del 4 agosto 2011);
- al personale di IS Roma Sicurezza, compreso quello che opera nella sala monitor, non è stata consegnata lettera di incarico in relazione all'attività effettuata presso FNAC (cfr. dichiarazioni rese nei verbali del 4 agosto 2011 e del 3 ottobre 2011), né sono stati designati incaricati del trattamento, né consta che agli stessi siano state impartite istruzioni circa le operazioni di trattamento effettuate, in difformità da quanto previsto dall'art. 30 del Codice;

- il personale di IS Roma Sicurezza in servizio presso la società, inoltre, non è risultato in possesso del decreto di riconoscimento della qualifica di guardia particolare giurata di cui all'art. 134, R.D. 18 giugno 1931, n. 773 (TULPS) (cfr. verbale 4 agosto 2011);

- diversamente da quanto prescritto nel menzionato accordo con le rappresentanze sindacali – secondo il quale le riprese effettuate "saranno custodite in un apposito armadio di sicurezza dotato di una doppia serratura", con consegna di due distinte chiavi, rispettivamente, al responsabile della sicurezza del negozio e alla RSA delegata del negozio, sì che "l'apertura dell'armadio sarà [...] consentita solo alla presenza contemporanea sia di un rappresentante dei lavoratori che di uno dell'azienda", con conservazione delle chiavi "in apposita busta sigillata, con la firma delle due figure delegate" –, è stato dichiarato che "l'accesso ai dati [registrati mediante il sistema di videosorveglianza] è possibile solo attraverso una password custodita dall'azienda che fa manutenzione all'impianto (FGS di Brescia), la quale viene contattata quando è necessario procedere alla visualizzazione di immagini precedentemente registrate", previa comunicazione di un codice personale da parte del responsabile della sicurezza (cfr. verbale 3 ottobre 2011);

- gli avvisi relativi al sistema di videosorveglianza sono risultati:

- presenti solo in talune delle aree riprese, in particolare sulla porta di accesso all'area di vendita e, mediante due cartelli informativi (uno dei quali non agevolmente visibile, essendo collocato dietro una struttura fissa preordinata all'esposizione della merce posta in vendita) situati al piano terreno e al piano seminterrato nonché

- sprovvisti dell'indicazione della finalità del trattamento (cfr. avviso allegato al verbale del 3 ottobre 2011 e immagine fotografica in atti);

VISTO il riscontro alla richiesta di informazioni inviata dall'Ufficio del Garante con il quale il legale rappresentante di FNAC Italia s.p.a., con nota del 28 dicembre 2011, ha dichiarato che:

- titolare dei trattamenti di dati personali effettuati mediante i sistemi di videosorveglianza operanti presso tutti gli esercizi commerciali presenti sul territorio è FNAC Italia s.p.a.;

- CIS s.p.a. – Consorzio Sicurezza Italia, unitamente alle società consorziate – e tra queste IS Roma Sicurezza – ha sottoscritto con FNAC Italia un contratto di appalto di servizi (il cui oggetto specifico, con riguardo alle prestazioni dovute, non si evince dalla documentazione prodotta in atti: cfr. "bozza 5 luglio 2011 - contratto di appalto per la fornitura di servizi", allegata alla comunicazione elettronica della Polizia di Stato del 2 dicembre 2011), in corrispondenza del quale, in data 16 maggio 2011, CIS e le società consorziate sono stati designati quali responsabili del trattamento dei dati personali effettuato mediante sistemi di videosorveglianza (cfr. atto di designazione di CIS prodotto da FNAC in allegato alla comunicazione del 28 dicembre 2011);

RILEVATO inoltre che l'area in cui è collocato il sistema di rilevazione delle presenze – situata in prossimità di un accesso di servizio – è ripresa da una telecamera che consente il controllo a distanza dell'attività dei lavoratori;

CONSIDERATO che il Garante ha affermato che "nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa, pertanto è vietata l'installazione di apparecchiature specificatamente preordinate alla predetta finalità: non devono quindi essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul badge)" (cfr. punto 4.1., Prov. 8 aprile 2010, cit.; v. altresì Prov. 10 novembre 2011, n. 421, doc. web n. [1859539](#));

RILEVATO che il sistema di rilevazione delle presenze deve essere collocato in un'area non interessata dalle riprese, in modo tale da consentire, in conformità all'art. 11, comma 1, lett. d), del Codice, il trattamento delle sole immagini pertinenti e non eccedenti rispetto alle finalità dichiarate dalla Società nonché esplicitate nel menzionato accordo sindacale adottato ai sensi dell'art. 4, comma 2, l. n. 300/1970;

RITENUTO, pertanto, di dover disporre il blocco del trattamento dei dati effettuato mediante la telecamera che riprende anche l'area nella quale è posta l'apparecchiatura per la rilevazione delle presenze dei lavoratori, in attesa dell'adozione delle misure idonee a prevenire tali riprese;

RITENUTO, inoltre, che la possibilità (dal punto di vista tecnico) per la Società di accedere alle immagini registrate, con l'ausilio di FGS di Brescia (soggetto che non risulta essere stato designato responsabile del trattamento), con modalità diverse da quelle stabilite nell'accordo con le rappresentanze sindacali si pone in violazione dei principi di liceità e correttezza nel trattamento (art. 11, comma 1, lett. a) e 4, comma 2, l. n. 300/1970);

CONSIDERATO altresì che, in base all'art. 134, R.D. 18 giugno 1931, n. 773 (TULPS) "senza licenza del Prefetto è vietato ad enti o privati di prestare opere di vigilanza o custodia di proprietà mobiliari od immobiliari [...]" (v. altresì l'art. 256-bis, R.D. 6 maggio 1940, n. 635, Approvazione del regolamento per l'esecuzione del testo unico 18 giugno 1931, n. 773 delle leggi di pubblica sicurezza, che specifica gli ambiti nei quali l'attività di vigilanza e custodia deve essere effettuata da guardie particolari giurate);

RILEVATO che, in base agli elementi in atti, il personale di IS Roma Sicurezza effettua presso la società attività riconducibili sia al servizio antitaccheggio (cfr. art. 3, comma 2, lett. d), D.M. 1° dicembre 2010, n. 269, Regolamento recante disciplina delle caratteristiche minime del progetto organizzativo e dei requisiti minimi di qualità degli istituti e dei servizi di cui agli articoli 256-bis e 257-bis del Regolamento di esecuzione del Testo unico delle leggi di pubblica sicurezza, nonché dei requisiti professionali e di capacità tecnica richiesti per la direzione dei medesimi istituti e per lo svolgimento di incarichi organizzativi nell'ambito degli stessi istituti) sia al servizio di televigilanza (cfr. art. 3, comma 2, lett. f), D.M. n. 269/2010), servizi che devono essere disimpegnati dagli istituti di vigilanza privata per mezzo delle dipendenti guardie giurate (cfr., rispettivamente, punti 3.h e 3.d, All. D, D.M. n. 269/2010, cit.);

RILEVATO che, anche di recente, la Corte di Cassazione (Cass. pen., sez. III, 3 dicembre 2010, n. 1821), nel richiamare il proprio indirizzo interpretativo ritenuto "assolutamente consolidato", ha ribadito che "ogni forma di attività imprenditoriale di vigilanza e custodia di beni per conto terzi esige la licenza del prefetto, indipendentemente dalle modalità operative con le quali viene espletata (sez. I, 28.4.1997 n. 3032, Montelli, RV 207684; sez. 5 2.3.1998 n. 1274, Mennuni, RV 210253; sez. 1, 12.1.2000 n. 191, Schinco, RV 215365; sez. 3, 17.10.2002 n. 42204, Montelli, RV 223600; sez. 1, 6.11.2008 n. 47742, Bellei, RV 242745; sez. 3, 16.12.2009 n. 1605 del 2010, Prowidenti, RV 245868)";

CONSIDERATO quindi illecito il trattamento di dati personali per finalità antitaccheggio effettuato mediante il descritto sistema di videosorveglianza da parte di soggetti non autorizzati ad effettuare tale attività visionando le immagini riprese sia presso la sede della Società, sia da remoto (art. 11, comma 1, lett. a), del Codice);

RITENUTO che, alla luce degli elementi sopra rappresentati, il descritto trattamento risulta effettuato dalla Società sotto più profili in violazione della disciplina di protezione dei dati personali (artt. 11, comma 1, lett. a) e d), 30 e 114 del Codice) (cfr. Provv.ti 14 aprile 2011, doc. web n. [1810223](#); 24 giugno 2010, doc. web n. [1738396](#); 26 febbraio 2009, doc. web n. [1601522](#));

CONSIDERATO che, ai sensi degli artt. 143, comma 1, lett. c) e 154, comma 1, lett. d), del Codice, il Garante ha il compito di disporre il blocco in caso di trattamento di dati illecito o non corretto;

RITENUTO, in attesa dell'adozione di idonee misure volte a rendere conforme al quadro normativo vigente il trattamento effettuato mediante il sistema di videosorveglianza esistente presso la sede di Genova della Società, di dover disporre il blocco di detto trattamento;

CONSIDERATO, inoltre, che gli avvisi sintetici affissi nei locali della società risultano sprovvisti dell'indicazione relativa alla finalità del trattamento e sono presenti solo in corrispondenza di talune delle aree riprese, diversamente da quanto indicato al punto 3.1. del menzionato provvedimento in materia di videosorveglianza dell'8 aprile 2010;

RITENUTO pertanto di dover prescrivere alla società, ai sensi degli artt. 143, comma 1, lett. b), e 154, comma 1, lett. c), del Codice, al fine di rendere il suddetto trattamento conforme alla disciplina in materia di protezione dei dati personali, l'adozione di misure e accorgimenti a garanzia degli interessati (fatti salvi quelli eventualmente già adottati, anche in conformità al provvedimento generale in materia di videosorveglianza dell'8 aprile 2010), e segnatamente di:

a. designare quale responsabile del trattamento, ai sensi dell'art. 29 del Codice, con riferimento alle operazioni che possono essere legittimamente effettuate, anche alla luce dell'accordo in essere con le rappresentanze sindacali, il soggetto cui è rimessa l'esecuzione di attività di trattamento di dati personali (quali quelle di manutenzione e, se del caso, di estrazione di copia delle immagini registrate);

b. integrare gli avvisi recanti l'informativa di cui all'art. 13 del Codice in forma "semplificata" con le informazioni indicate nel provvedimento generale dell'8 aprile 2010 (al punto 3.1.), con formato e posizionamento tali da essere chiaramente visibili;

RISERVATA la valutazione da parte dell'Autorità, con autonomo procedimento, della sussistenza di violazioni amministrative in capo al titolare del trattamento;

RITENUTO di disporre la trasmissione degli atti e di copia del presente provvedimento all'autorità giudiziaria per le valutazioni di competenza in ordine agli illeciti penali che riterrà eventualmente configurabili;

RILEVATO che, in caso di inosservanza del presente provvedimento, si renderanno applicabili le sanzioni di cui agli artt. 162, comma 2-ter e 170 del Codice;

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

RELATORE la prof.ssa Licia Califano;

TUTTO CIÒ PREMESSO, IL GARANTE

nei confronti di FNAC Italia s.p.a.:

1. dichiara illecito, nei termini di cui in motivazione, il trattamento effettuato a mezzo del sistema di videosorveglianza installato presso l'esercizio commerciale di Genova, con la conseguente inutilizzabilità dei dati trattati in violazione di legge ai sensi dell'art. 11, comma 2 del Codice e, in attesa dell'adozione di idonee misure volte a rendere conforme al quadro normativo vigente il trattamento effettuato, ai sensi degli artt. 143, comma 1, lett. c), 144 e 154, comma 1, lett. d), del Codice, dispone il blocco del trattamento dei dati personali effettuato mediante lo stesso;

2. ai sensi degli artt. 143, comma 1, lett. c), 144 e 154, comma 1, lett. d), del Codice, dispone il blocco del trattamento dei dati personali effettuato mediante la telecamera che riprende anche l'area nella quale è posta l'apparecchiatura per la rilevazione delle presenze dei lavoratori, in attesa dell'adozione delle misure idonee a prevenire tali riprese;

3. prescrive, ai sensi degli artt. 143, comma 1, lett. b), 144 e 154, comma 1, lett. c) del Codice, senza ritardo, e comunque entro trenta giorni dal ricevimento del presente provvedimento, di:

a. designare quale responsabile del trattamento, ai sensi dell'art. 29 del Codice, con riferimento alle operazioni che possono

essere legittimamente effettuate, anche alla luce dell'accordo in essere con le rappresentanze sindacali, il soggetto cui è rimessa l'esecuzione di attività di trattamento di dati personali;

b. integrare gli avvisi recanti l'informativa "semplificata" con le informazioni indicate al punto 3.1. del provvedimento generale dell'8 aprile 2010, con formato e posizionamento tali da essere chiaramente visibili;

4. ai sensi dell'art. 157 del Codice, invita la società a dare comunicazione al Garante delle misure adottate entro 30 giorni dalla data di ricezione del presente provvedimento;

5. dispone la trasmissione degli atti e di copia del presente provvedimento all'autorità giudiziaria per le valutazioni di competenza in ordine agli illeciti penali che riterrà eventualmente configurabili.

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, 17 gennaio 2013

IL PRESIDENTE
Soro

IL RELATORE
Califano

IL SEGRETARIO GENERALE
Busia