2. PROVVEDIMENTI E NORMATIVA DEL GARANTE DELLA PRIVACY

SOMMARIO:

2.1. Verifica preliminare. Sistemi di videosorveglianza dotati di software "intelligent video" - 17 marzo 2016

Registro dei provvedimenti
n. 127 del 17 marzo 2016

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 prof.ssa Licia Califano e della dott.ssa Giovanna Bianchi Clerici, componenti, e del dott. Giuseppe Busia, segretario generale;

Esaminata la richiesta di verifica preliminare presentata da LFoundry S.r.l. ai sensi dell'art. 17 del d.lg. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, di seguito Codice);

Visto il provvedimento generale in materia di videosorveglianza dell'8 aprile 2010 (in www.gdpd.it; doc. web n. 1712680), con particolare riferimento al punto 3.4;

Esaminata la documentazione acquisita agli atti;

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;

PREMESSO

1. L'istanza della società.

In data 15 luglio 2015, LFoundry S.r.l., in ossequio a quanto prescritto dal provvedimento in materia di videosorveglianza dell'8 aprile 2010, ha fatto pervenire un'istanza di verifica preliminare (art. 17 del Codice) –regolarizzata con nota del 6 ottobre 2015- al fine di poter istallare un nuovo impianto di videosorveglianza, presso la propria sede ubicata ad Avezzano, dotato di software "intelligent video" e poter conservare le relative immagini per un periodo di 45 giorni, al fine di conformarsi agli elevati standard di qualità e sicurezza richiesti dal proprio mercato di riferimento.

La Società, che opera nel settore dei semiconduttori, offrendo servizi di design e "manifattura di dispositivi a semiconduttore", ultimamente ha ampliato il proprio ambito di attività anche nel comparto delle "smart card", attraverso la produzione di "dispositivi destinati a SIM, POS, terminal applications, credit cards, ePassport etc…", prodotti che appartengono tutti al cosiddetto comparto "secure" che richiede elevati requisiti di sicurezza (cfr. nota del 15 luglio 2015).

Lo stabilimento produttivo di Avezzano, ubicato nella zona industriale della città, si sviluppa su una vasta superficie ed è composto da diversi edifici fra cui: un fabbricato dove sono collocati gli uffici, i laboratori e il magazzino; una struttura comprendente l'area di produzione vera e propria; un'area riservata alla distribuzione e allo stoccaggio dei prodotti chimici; una centrale di cogenerazione; un impianto per il trattamento delle acque reflue; un'area per lo stoccaggio temporaneo dei rifiuti.

All'interno del perimetro di LFoundry S.r.l., risiedono anche altre due aziende che si occupano rispettivamente di "produzione di dispositivi a semiconduttore" (Micron Semiconductor Italia S.r.l.) e produzione di "gas utilizzati nei processi produttivi di LFoundry" (Air Product Italia S.r.l.). Al riguardo, è stato specificato che queste due aziende, fornitrici di materiali a favore di LFoundry S.r.l. e per le quali la stessa Società svolge un servizio di vigilanza (cfr. nota del 6 ottobre 2015), "costituiscono un elemento di rischio aggiuntivo", sia per la natura che per le tipologie di lavorazioni effettuate (cfr. nota del 15 luglio 2015).

In ragione delle attività lavorative eseguite, lo stabilimento è in possesso, tra l'altro, di un'autorizzazione specifica per "detenzione ed impiego di gas tossici", rilasciata dal Comune di Avezzano e di un "Nulla osta alla detenzione ed impiego di sorgenti di radiazioni ionizzanti", rilasciato dalla Prefettura, mentre tutto il sito produttivo è classificato come "a rischio di incidente rilevante ai sensi dell'art. 6 e 7 del d.lgs. n. 334/99" che ha recepito la Direttiva 96/82/CE e successive integrazioni e modificazioni.

Le aree del sito sono accessibili secondo quattro livelli di accesso, in ragione della criticità degli impianti, dei prodotti e delle informazioni che contengono.

In particolare, la nuova attività svolta da LFoundry S.r.l. nel cosiddetto comparto "secure", ha spinto la stessa azienda ad intraprendere un percorso ufficiale di valutazione dello stabilimento di Avezzano presso l'Organismo di Certificazione della Sicurezza Informatica (OCSI), che gestisce lo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, al fine di ottenere la certificazione nel rispetto delle previsioni dettate dai Common Criteria (standard ISO/IEC 15408).

Per ciò che riguarda l'impianto di videosorveglianza, la Società ha dichiarato che lo stesso è stato realizzato per assolvere funzioni di safety e security, essendo rivolto sia alla sicurezza del personale sia alla tutela del patrimonio aziendale, di cui fanno parte anche le zone date "in comodato d'uso" alle altre aziende citate.

Ciò premesso, LFoundry S.r.l. ha sostenuto che la ragione della richiesta di verifica preliminare, volta alla realizzazione di un sistema dotato di software "intelligent video" ed alla conservazione delle relative immagini per un periodo di 45 giorni, risiederebbe non solo nell'esigenza di rafforzare in termini generali il livello di tutela del sito, anche in considerazione di alcuni episodi criminosi relativi ad intrusioni e furti, regolarmente denunciati (cfr. nota del 6 ottobre 2015), ma anche quella di soddisfare i requisiti richiesti dai predetti Common Criteria che presuppongono la necessità di revisionare i sistemi di sicurezza del sito produttivo di Avezzano e con ciò anche il sistema di videosorveglianza presente.

Riguardo al rispetto della normativa in materia di controllo a distanza sull'attività lavorativa, la Società ha dichiarato di aver osservato la procedura prevista dall'art. 4, comma 2, della legge n. 300/1970, siglando con le RSU dello stabilimento successivi accordi sindacali in ragione delle varie modifiche intervenute sull'impianto.

2. Le modalità di funzionamento del sistema

L'impianto di videosorveglianza di cui la Società già si avvale è affiancato da un sistema di controllo accessi per l'ingresso alle aree riservate ed è provvisto di 142 videocamere (analogiche e digitali) dislocate sia all'interno dei vari edifici che compongono il sito, sia all'esterno; di queste 12 sono di tipo PTZ, caratterizzate cioè da uno zoom ottico e dalla possibilità di movimentazione dell'apparecchio sia in verticale che in orizzontale, le altre di tipo fisso (cfr. nota 15 luglio 2015).

Per ciò che riguarda l'angolo di visuale delle telecamere è stato riferito che solamente le aree di lavoro ad accesso controllato, e cioè quelle relative allo stoccaggio dei prodotti secure, nonché "i locali motori" e quelli adibiti "allo stoccaggio e distribuzione di gas tossici e sostanze pericolose" sono costantemente monitorate, per il resto, le inquadrature riguardano solamente aree di transito (parcheggi e piazzole di sosta) e varchi di accesso.

Le immagini, registrate su alcuni server collocati all'interno di un locale tecnico e convogliate tramite una rete dedicata presso la sala controllo security, sono visionabili in live solamente dalle Guardie Particolari Giurate (GPG), designate incaricate del trattamento.

L'accesso alle immagini registrate, attualmente conservate solo per 7 giorni all'interno del locale tecnico, è consentito solamente per esigenze di manutenzione degli apparati di videosorveglianza e a seguito dell'accadimento di fatti illeciti. Tale accesso è riservato ad un "ristretto numero di soggetti", designati incaricati del trattamento, secondo il principio del "need to know" (che implica il privilegio di accedere alle immagini nella misura minima necessaria per svolgere le proprie mansioni), tramite un sistema di "strong authentication".

Infine, per quanto riguarda l'obbligo di rendere l'informativa, LFoundry S.r.l., titolare del trattamento dei dati, ha dichiarato di aver affisso la specifica cartellonistica presso la struttura (cfr. nota del 15 luglio 2015).

Secondo gli intendimenti manifestati dalla società con la richiesta in esame, il progetto di revisione dell'impianto di videosorveglianza, da implementare anche in ragione degli elevati standard di sicurezza richiesti nel comparto "secure" (dove la Società ha cominciato ad operare), comporterebbe tre tipi di integrazioni. La prima consisterebbe in un potenziamento del sistema antintrusione (espressamente richiesto a seguito dell'audit sul sistema di sicurezza della Società, effettuato da un laboratorio accreditato dall'organismo francese ANSSI, per conto di uno dei clienti della Società), con l'aggiunta di 19 videocamere termiche perimetrali, 4 apparecchi ottici per il controllo accessi ai varchi di ingresso, 1 videocamera per il riconoscimento delle targhe dei veicoli in ingresso al sito, 1 server aggiuntivo e un software di "intelligent video" a protezione della proprietà.

In particolare, le telecamere termiche, poste lungo il perimetro, non essendo in grado di effettuare alcuna identificazione, avrebbero la funzione di attivare l'allarme in sala controllo e conseguentemente anche l'eventuale intervento delle G.P.G. presenti nel sito, a seguito dell'individuazione di forme in movimento all'interno dell'area identificata come "no access zone".

Le telecamere ottiche, dotate del predetto sofware, avrebbero, invece, l'obiettivo di controllare la situazione laddove è necessario consentire l'accesso agli autoveicoli e cioè ai varchi di accesso "Visitatori", "Dipendenti" e "Merci", di per sé privi di presidio. Il meccanismo effettuerebbe, perciò, una discriminazione "tra accessi leciti ed accessi illeciti", rilevando il verificarsi di accessi pedonali non autorizzati ai varchi riservati ai veicoli. Inoltre, in prossimità del solo "Ingresso Dipendenti" sarebbe anche collocata la videocamera per il riconoscimento delle targhe che, in azione congiunta con una sbarra, avrebbe lo scopo di consentire l'accesso ai soli veicoli censiti come autorizzati.

L'accesso di altri veicoli non censiti ma autorizzati sarebbe garantita, previa identificazione, presso altri ingressi.

La seconda parte del progetto, riguarderebbe l'allungamento dei tempi di conservazione delle immagini registrate fino a 45 giorni al fine di permettere la ricostruzione di eventuali episodi anomali segnalati.
Infine, la terza integrazione consisterebbe nell'implementazione di un ulteriore software "intelligent video" da collocare in prossimità di tutte le zone ad alto rischio ed in grado di assolvere sia una funzione di protezione Safety (cioè nei confronti del personale), sia Security (cioè nei confronti del patrimonio); ciò, attraverso il posizionamento di alcune telecamere munite di sistema di riconoscimento di "pattern comportamentale", in grado di individuare condizioni anomale, "quali la rilevazione di un uomo a terra" o "lo stato di immobilità di una persona" per un certo tempo (cfr. nota del 6 ottobre 2015), oppure condizioni di "loitering, manomissione" o sottrazione di materiali, e conseguentemente allarmare la sala di controllo, garantendo l'intervento tempestivo delle squadre di soccorso o delle guardie giurate a seconda dell'evento occorso (cfr. nota del 15 luglio 2015).

3. Presupposti di liceità del trattamento

Per una corretta valutazione dell'istanza occorre necessariamente tenere conto della peculiarità della fattispecie e, in particolare, del fatto che la realizzazione di un sistema dotato di software "intelligent video" e la conservazione delle relative immagini per un periodo di 45 giorni, è determinata in particolar modo dall'esigenza di uniformarsi ai parametri di sicurezza che trovano origine nel proprio mercato di riferimento ed in particolare negli stringenti criteri dettati dallo standard ISO/15408, che fissa i cosiddetti "Common Criteria" (volti a verificare la sicurezza dei sistemi o dei prodotti sulla base degli "obiettivi" cui essi sono preordinati, del contesto del loro impiego e delle pregresse verifiche di sicurezza su di essi eseguite); il maggiore o minore rispetto di tali standard di sicurezza incide sul conseguente livello di valutazione EAL ("Evaluation Assurance Level"), che secondo gli intendimenti della Società dovrebbe essere "+5".
Per ciò che riguarda il valore legale delle norme tecniche "ISO" (che sono definite dalla International Organization for Standardization, di cui sono membri 157 organismi nazionali di standardizzazione, tra cui l'Ente Nazionale Italiano di Unificazione-UNI), occorre rilevare che la Direttiva 98/34/CE del Parlamento europeo e del Consiglio del 22/06/1998 (che prevede "una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione"), all'art. 1, n. 6 definisce "norma" una specificazione tecnica che, pur non essendo obbligatoria, sia stata approvata, in vista di una sua applicazione ripetuta o continuativa, da parte di un organismo "riconosciuto ad attività normativa", e precisamente da un'organizzazione internazionale, europea o nazionale di normalizzazione che l'abbia posta "a disposizione del pubblico". Pertanto, le norme ISO (così come quelle EN a livello europeo e quelle UNI per l'Italia) rappresentano "specificazioni tecniche" che forniscono standard qualitativi contemplati da documenti che, in ragione delleconoscenze tecniche di un determinato momento storico, definiscono le caratteristiche (dimensionali, prestazionali, ambientali, di sicurezza, di organizzazione, ecc.) di un prodotto, di un processo o di un servizio.
Ciò premesso, benché tali norme non siano giuridicamente vincolanti, non può non tenersi conto del fatto che esse si riferiscono a settori di rilevante interesse pubblico e, al contempo, tecnologicamente assai complessi, tanto che spesso sono le stesse autorità pubbliche a promuoverne l'osservanza o, addirittura, a fare diretto riferimento ad esse ; inoltre, anche sul piano privatistico, va sottolineata l'esistenza di una consolidata prassi al loro inserimento all'interno degli schemi contrattuali nazionali ed esteri, espressione di una progressiva trasformazione dei mercati e della connessa evoluzione degli standard di sicurezza in senso sovranazionale. Ne deriva che non può disconoscersi che alle specifiche tecniche in esame, di fatto, venga oramai generalmente attribuita una valenza di gran lunga superiore rispetto a quella che dovrebbe loro spettare in ragione delle modalità di adozione, sicché gli standard di sicurezza da esse fissati possono ritenersi oramai considerati –sia in sede nazionale, sia in sede internazionale- come un punto di riferimento ineludibile in occasione della fornitura di opere o della prestazione di servizi ad alto contenuto tecnologico.

Tutto ciò premesso, nel delicato settore in cui opera Lfoundry S.r.l. trovano applicazione le specifiche tecniche contenute nella ISO/15408, volte a garantire determinati standard di sicurezza in vista della realizzazione di sistemi o prodotti ITC.
Nell'ambito di tali standard può essere ricondotta la scelta della Società di installare all'interno dei siti produttivi adeguati sistemi di videosorveglianza, al fine di proteggere i propri dipendenti ma anche di prevenire accessi non autorizzati o danneggiamenti al patrimonio aziendale, comprendente informazioni, strutture e materiali.
Per ciò che riguarda l'implementazione dei sistemi di intelligent video sopra descritti, essi debbono essere valutati alla luce dei principi di necessità, proporzionalità, finalità e correttezza posti dal Codice (artt. 3 e 11 del Codice), espressamente richiamati anche nel Provvedimento generale in materia di videosorveglianza dell'8 aprile 2010.
In particolare, secondo tale provvedimento "in linea di massima tali sistemi devono considerarsi eccedenti rispetto alla normale attività di videosorveglianza , in quanto possono determinare effetti particolarmente invasivi sulla sfera di autodeterminazione dell'interessato e, conseguentemente, sul suo comportamento. Il relativo utilizzo risulta comunque 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" posti dai citati artt. 3 e 11 del Codice.
In ragione di ciò, si ritiene che, innanzitutto, sia importante tenere in debito conto il particolare ambito di attività di LFoundry S.r.l., giacché nello stabilimento di Avezzano, classificato a rischio incidente rilevante, vengono prodotti delicati componenti elettronici, che oltre ad essere impiegati nel settore delle telecomunicazioni e dell'informatica, rivestono un ruolo fondamentale per la realizzazione di "dispositivi destinati a SIM, POS, terminal applications, credit cards, ePassport etc, cui sono connesse forti esigenze di salvaguardia, essendo destinati ad operare all'interno di sistemi di identificazione sicura sia in ambito pubblico, sia in ambito privato.
In tal senso, l'implementazione di un sistema intelligent video avrebbe non solo un'importante funzione di tutela della salute ed incolumità dei lavoratori, ma anche di salvaguardia delle attività economiche effettuate al suo interno.
In secondo luogo, vanno poste in evidenza l'ubicazione dello stabilimento di LFoundry S.r.l., adiacente a vie di fuga facilmente raggiungibili, l'ampiezza del sito e la presenza di altre strutture all'interno del perimetro dell'azienda per le quali la stessa LFoundry S.r.l. svolge attività di sorveglianza, che per tipologia di lavorazioni effettuate "costituiscono un elemento di rischio aggiuntivo". Rischiosità che trova del resto conferma negli eventi delittuosi verificatisi in passato nello stabilimento medesimo, regolarmente denunciati dalla società alle autorità.
Tali obiettive circostanze già permettono di ritenere che il sito in questione sia caratterizzato da peculiarità che giustificano l'adozione di standard di sicurezza di livello superiore alla media.
Per quanto riguarda la richiesta di allungare il termine di conservazione delle immagini videoregistrate, il Provvedimento generale in materia di videosorveglianza dell'8 aprile 2010 prevede che l'allungamento dei tempi di conservazione dei dati oltre i sette giorni, deve essere adeguatamente motivato "con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità.
Nel caso in questione, la società ha dichiarato che il livello di certificazione Eal 5+, a cui la stessa ambisce, si riferisce all'intera "catena di fornitori" (supply chain) del prodotto oggetto di certificazione; con la conseguenza che nel caso in questione LFoundry S.r.l. si trova ad essere "responsabile contrattualmente anche delle attività di lavorazione" svolte presso un sub-contractor, essendo con ciò tenuta ad accertare eventuali violazioni dei protocolli di sicurezza sia nel proprio ciclo produttivo che in quello demandato ad aziende esterne.
Ciò premesso, la richiesta di allungamento dei tempi di conservazioni delle immagini fino a 45 giorni avrebbe il pregio di permettere all'azienda di ricostruire quanto eventualmente accaduto nel sito produttivo, in caso di anomalie segnalate da un soggetto della catena di fornitura a valle dello stabilimento, dal momento che il tempo complessivo intercorrente dal momento in cui il prodotto

esce dallo stabilimento a quello in cui è disponibile al cliente sul mercato "non è inferiore a 5 settimane".
Ad avviso di questa Autorità, all'esito dell'istruttoria sono emersi elementi che inducono a ritenere che la richiesta della società possa essere accolta perché conforme ai principi posti dagli artt. 3 e 11 del Codice.
In particolare, l'ubicazione isolata del sito, il delicato settore produttivo in cui opera LFoundry S.r.l. e la specifica attenzione posta non solo a livello internazionale ed europeo, ma anche a livello nazionale rispetto alla fissazione e alla comune osservanza di elevati standard di sicurezza nella produzione di beni e servizi relativi al settore elettronico ed informatico, valgono a giustificare la pretesa di procedere all'installazione dei predetti sistemi di intelligent video ed alla relativa conservazione dei dati per 45 giorni, all'esclusivo fine dell'accertamento degli accadimenti e dell'individuazione degli eventuali responsabili di fatti illeciti.
Resta inteso che, ad eccezione della visione da parte dell'Autorità giudiziaria, l'accesso alle immagini in questione potrà avvenire solo nel rispetto di quanto stabilito dagli accordi sindacali aziendali, con conseguente divieto di loro comunicazione a terzi (fatte salve le esigenze dell'Autorità giudiziaria) o di diffusione.
TUTTO CIÒ PREMESSO IL GARANTE
ai sensi dell'art. 17 del Codice, a conclusione della verifica preliminare ammette l'utilizzo dei sistemi di videosorveglianza dotati di software "intelligent video" e la conservazione delle relative immagini per un periodo di 45 giorni da parte di LFoundry S.r.l., nelle forme e nei limiti di cui in motivazione.
Roma, 17 marzo 2016
IL PRESIDENTE
Soro
IL RELATORE
Califano
IL SEGRETARIO GENERALE
Busia

2.2. Provvedimento in materia di videosorveglianza - 8 aprile 2010

(Gazzetta Ufficiale n. 99 del 29 aprile 2010)

Sommario

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Daniele De Paoli, segretario generale reggente;

VISTO lo schema del provvedimento in materia di videosorveglianza approvato dal Garante il 22 dicembre 2009 e trasmesso al Ministero dell'Interno, all'Unione delle Province d'Italia (UPI) ed all'Associazione Nazionale Comuni Italiani (ANCI), al fine di acquisirne preventivamente le specifiche valutazioni per i profili di competenza;

CONSIDERATE le osservazioni formulate dall' ANCI con note del 25 febbraio 2010 (prot. n. 10/Area INSAP/AR/crc-10) e del 29 marzo 2010 (prot. n. 17/*Area* INSAP/AR/a*r*-10);

CONSIDERATE le osservazioni formulate dal Ministero dell'Interno con nota del 26 febbraio 2010;

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

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

Relatore il prof. Francesco Pizzetti;

1. PREMESSA

Il trattamento dei dati personali effettuato mediante l'uso di sistemi di videosorveglianza non forma oggetto di legislazione specifica; al riguardo si applicano, pertanto, le disposizioni generali in tema di protezione dei dati personali.

Il Garante ritiene necessario intervenire nuovamente in tale settore con il presente provvedimento generale che sostituisce quello del 29 aprile 2004 (1).

Ciò in considerazione sia dei numerosi interventi legislativi in materia, sia dell'ingente quantità di quesiti, segnalazioni, reclami e richieste di verifica preliminare in materia sottoposti a questa Autorità.

Nel quinquennio di relativa applicazione, infatti, talune disposizioni di legge hanno attribuito ai sindaci e ai comuni specifiche competenze volte a garantire l'incolumità pubblica e la sicurezza urbana(2), mentre altre norme, statali(3) e regionali(4), hanno previsto altresì forme di incentivazione economica a favore delle amministrazioni pubbliche e di soggetti privati al fine di

incrementare l'utilizzo della videosorveglianza quale forma di difesa passiva, controllo e deterrenza di fenomeni criminosi e vandalici.

2. TRATTAMENTO DEI DATI PERSONALI E VIDEOSORVEGLIANZA: PRINCIPI GENERALI

La raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configura un trattamento di dati personali (*art. 4, comma 1, lett. b), del Codice*). È considerato dato personale, infatti, qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

Un'analisi non esaustiva delle principali applicazioni dimostra che la videosorveglianza è utilizzata a fini molteplici, alcuni dei quali possono essere raggruppati nei seguenti ambiti generali:

1) protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine e sicurezza pubblica, alla prevenzione, accertamento o repressione dei reati svolti dai soggetti pubblici, alla razionalizzazione e miglioramento dei servizi al pubblico volti anche ad accrescere la sicurezza degli utenti, nel quadro delle competenze ad essi attribuite dalla legge;

2) protezione della proprietà;

3) rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge;

4) acquisizione di prove.

La necessità di garantire, in particolare, un livello elevato di tutela dei diritti e delle libertà fondamentali rispetto al trattamento dei dati personali consente la possibilità di utilizzare sistemi di videosorveglianza, purché ciò non determini un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli interessati.

Naturalmente l'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili, quali ad es. le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata(5), sul controllo a distanza dei lavoratori(6), in materia di sicurezza presso stadi e impianti sportivi(7), o con riferimento a musei, biblioteche statali e archivi di Stato(8), in relazione ad impianti di ripresa sulle navi da passeggeri adibite a viaggi nazionali(9) e, ancora, nell'ambito dei porti, delle stazioni ferroviarie, delle stazioni delle ferrovie metropolitane e nell'ambito delle linee di trasporto urbano(10).

In tale quadro, pertanto, è necessario che:

a) il trattamento dei dati attraverso sistemi di videosorveglianza sia fondato su uno dei presupposti di liceità che il Codice prevede espressamente per i soggetti pubblici da un lato (svolgimento di funzioni istituzionali: *artt. 18-22 del Codice*) e, dall'altro, per soggetti privati ed enti pubblici economici (es. adempimento ad un obbligo di legge, provvedimento del Garante di c.d. "bilanciamento di interessi" -v., in proposito, punto 6.2- o consenso libero ed espresso: *artt. 23-27 del Codice*). Si tratta di presupposti operanti in settori diversi e che sono pertanto richiamati separatamente nei successivi paragrafi del presente provvedimento relativi, rispettivamente, all'ambito pubblico e a quello privato;

b) ciascun sistema informativo ed il relativo programma informatico vengano conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi (es., configurando il programma informatico in modo da consentire, per monitorare il traffico, solo riprese generali che escludano la possibilità di ingrandire le immagini e rendere identificabili le persone). Lo impone il *principio di necessità*, il quale comporta un obbligo di attenta configurazione di sistemi informativi e di programmi informatici per ridurre al minimo l'utilizzazione di dati personali (*art. 3 del Codice*);

c) l'attività di videosorveglianza venga effettuata nel rispetto del c.d. principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite (*art. 11, comma 1, lett. d) del Codice*).

3. ADEMPIMENTI APPLICABILI A SOGGETTI PUBBLICI E PRIVATI

3.1.Informativa

Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (es. concerti, manifestazioni sportive).

A tal fine, il Garante ritiene che si possa utilizzare lo stesso modello semplificato di informativa "minima", indicante il titolare del trattamento e la finalità perseguita, già individuato ai sensi dell'art. 13, comma 3, del Codice nel provvedimento del 2004 e riportato in *fac-simile* nell'allegato n. 1 al presente provvedimento.

Il modello è ovviamente adattabile a varie circostanze. In presenza di più telecamere, in relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, potranno essere installati più cartelli.

Il supporto con l'informativa:

• deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;

• deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;

• può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

Il Garante ritiene auspicabile che l'informativa, resa in forma semplificata avvalendosi del predetto modello, poi rinvii a un testo completo contenente tutti gli elementi di cui all'art. 13, comma 1, del Codice, disponibile agevolmente senza oneri per gli interessati, con modalità facilmente accessibili anche con strumenti informatici e telematici (in particolare, tramite reti Intranet o siti Internet, affissioni in bacheche o locali, avvisi e cartelli agli sportelli per gli utenti, messaggi preregistrati disponibili digitando un numero telefonico gratuito).

In ogni caso il titolare, anche per il tramite di un incaricato, ove richiesto è tenuto a fornire anche oralmente un'informativa adeguata, contenente gli elementi individuati dall'art. 13 del Codice.

3.1.1. Informativa e sicurezza

Talune disposizioni del Codice, tra le quali quella riguardante l'obbligo di fornire una preventiva informativa agli interessati, non sono applicabili al trattamento di dati personali effettuato, anche sotto forma di suoni e immagini, dal *"Centro elaborazione dati del Dipartimento di pubblica sicurezza o da forze di polizia sui dati destinati a confluirvi in base alla legge, ovvero da organi di pubblica sicurezza o altri soggetti pubblici per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati, effettuati in base ad espressa disposizione di legge che preveda specificamente il trattamento" (art. 53 del Codice)*.

Alla luce di tale previsione del Codice, i predetti titolari del trattamento di dati personali devono osservare i seguenti principi:

a) l'informativa può non essere resa quando i dati personali sono trattati per il perseguimento delle finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati;

b) il trattamento deve comunque essere effettuato in base ad espressa disposizione di legge che lo preveda specificamente.

3.1.2. Ulteriori specificazioni: l'informativa eventuale nella videosorveglianza effettuata per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati

Il Garante, al fine di rafforzare la tutela dei diritti e delle libertà fondamentali degli interessati, ritiene fortemente auspicabile che l'informativa, benché non obbligatoria, laddove l'attività di videosorveglianza sia espletata ai sensi dell'art. 53 del Codice, sia comunque resa in tutti i casi nei quali non ostano in concreto specifiche ragioni di tutela e sicurezza pubblica o di prevenzione, accertamento o repressione dei reati.

Ciò naturalmente all'esito di un prudente apprezzamento volto a verificare che l'informativa non ostacoli, ma anzi rafforzi, in concreto l'espletamento delle specifiche funzioni perseguite, tenuto anche conto che rendere palese l'utilizzo dei sistemi di videosorveglianza può, in molti casi, svolgere una efficace funzione di deterrenza.
A tal fine i titolari del trattamento possono rendere nota la rilevazione di immagini tramite impianti di videosorveglianza attraverso forme anche semplificate di informativa, che evidenzino, mediante l'apposizione nella cartellonistica di riferimenti grafici, simboli, diciture, l'utilizzo di tali sistemi per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati.
In ogni caso resta fermo che, anche se i titolari si avvalgono della facoltà di fornire l'informativa, resta salva la non applicazione delle restanti disposizioni del Codice tassativamente indicate dall'art. 53, comma 1, lett. *a*) e *b*).
Va infine sottolineato che deve essere obbligatoriamente fornita un'idonea informativa in tutti i casi in cui, invece, i trattamenti di dati personali effettuati tramite l'utilizzo di sistemi di videosorveglianza dalle forze di polizia, dagli organi di pubblica sicurezza e da altri soggetti pubblici non siano riconducibili a quelli espressamente previsti dall'art. 53 del Codice (es. utilizzo di sistemi di rilevazioni delle immagini per la contestazione delle violazioni del Codice della strada).

3.1.3. Informativa da parte dei soggetti privati che effettuano collegamenti con le forze di polizia

I trattamenti di dati personali effettuati da soggetti privati tramite sistemi di videosorveglianza, direttamente collegati con le forze di polizia, esulano dall'ambito di applicazione dell'art. 53 del Codice. Pertanto, l'attivazione del predetto collegamento deve essere reso noto agli interessati. A tal fine, il Garante ritiene che si possa utilizzare il modello semplificato di informativa "minima" - indicante il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia- individuato ai sensi dell'art. 13, comma 3, del Codice e riportato in *fac-simile* nell'allegato n. 2 al presente provvedimento. Nell'ambito del testo completo di informativa reso eventualmente disponibile agli interessati, tale collegamento deve essere reso noto.
Al predetto trattamento si applicano le prescrizioni contenute nel punto 4.6
La violazione delle disposizioni riguardanti l'informativa di cui all'art. 13, consistente nella sua omissione o inidoneità (es. laddove non indichi comunque il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia), è punita con la sanzione amministrativa prevista dall'art. 161 del Codice.
Le diverse problematiche riguardanti le competenze attribuite ai comuni in materia di sicurezza urbana sono esaminate al punto 5.1.

3.2. Prescrizioni specifiche

3.2.1.Verifica preliminare

I trattamenti di dati personali nell'ambito di una attività di videosorveglianza devono essere effettuati rispettando le misure e gli accorgimenti prescritti da questa Autorità come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello del titolare (*art. 17 del Codice*), quando vi sono 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.
In tali ipotesi devono ritenersi ricompresi i sistemi di raccolta delle immagini associate a dati biometrici. L'uso generalizzato e incontrollato di tale tipologia di dati può comportare, in considerazione della loro particolare natura, il concreto rischio del verificarsi di un pregiudizio rilevante per l'interessato, per cui si rende necessario prevenire eventuali utilizzi impropri, nonché possibili abusi.
Ad esempio, devono essere sottoposti alla verifica preliminare di questa Autorità i sistemi di videosorveglianza dotati di *software* che permetta il riconoscimento della persona tramite collegamento o incrocio o confronto delle immagini rilevate (es. morfologia del volto) con altri

specifici dati personali, in particolare con dati biometrici, o sulla base del confronto della relativa immagine con una campionatura di soggetti precostituita alla rilevazione medesima.
Un analogo obbligo sussiste con riferimento a sistemi 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, ed eventualmente registrarli. In linea di massima tali sistemi devono considerarsi eccedenti rispetto alla normale attività di videosorveglianza, in quanto possono determinare effetti particolarmente invasivi sulla sfera di autodeterminazione dell'interessato e, conseguentemente, sul suo comportamento. Il relativo utilizzo risulta comunque 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 (*artt. 3 e 11 del Codice*).
Deve essere sottoposto a verifica preliminare l'utilizzo di sistemi integrati di videosorveglianza nei casi in cui le relative modalità di trattamento non corrispondano a quelle individuate nei punti 4.6 e 5.4 del presente provvedimento.
Ulteriori casi in cui si rende necessario richiedere una verifica preliminare riguardano l'allungamento dei tempi di conservazione dei dati delle immagini registrate oltre il previsto termine massimo di sette giorni derivante da speciali esigenze di ulteriore conservazione, a meno che non derivi da una specifica richiesta dell'autorità giudiziaria o di polizia giudiziaria in relazione a un'attività investigativa in corso (v. punto 3.4).
Comunque, anche fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti individuati nel presente provvedimento non sono integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere una verifica preliminare a questa Autorità.

3.2.2. Esclusione della verifica preliminare

Il titolare del trattamento di dati personali effettuato tramite sistemi di videosorveglianza non deve richiedere una verifica preliminare purché siano rispettate tutte le seguenti condizioni:
a) il Garante si sia già espresso con un provvedimento di verifica preliminare in relazione a determinate categorie di titolari o di trattamenti;
b) la fattispecie concreta, le finalità del trattamento, la tipologia e le modalità d'impiego del sistema che si intende adottare, nonché le categorie dei titolari, corrispondano a quelle del trattamento approvato;
c) si rispettino integralmente le misure e gli accorgimenti conosciuti o concretamente conoscibili prescritti nel provvedimento di cui alla lett. *a*) adottato dal Garante.
Resta inteso che il normale esercizio di un impianto di videosorveglianza, non rientrante nelle ipotesi previste al precedente punto 3.2.1, non deve essere sottoposto all'esame preventivo del Garante, sempreché il trattamento medesimo avvenga con modalità conformi al presente provvedimento.
Resta altresì inteso che nessuna approvazione implicita può desumersi dal semplice inoltro al Garante di documenti relativi a progetti di videosorveglianza (spesso generici e non valutabili a distanza) cui non segua un esplicito riscontro dell'Autorità, in quanto non si applica il principio del silenzio-assenso.

3.2.3. Notificazione

E' regola generale che i trattamenti di dati personali devono essere notificati al Garante solo se rientrano in casi specificamente previsti (*art. 37 del Codice*). In relazione a quanto stabilito dalla lett. *f*), del comma 1, dell'art. 37, questa Autorità ha già disposto che non vanno comunque notificati i trattamenti di dati effettuati per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio ancorché relativi a comportamenti illeciti o fraudolenti, quando immagini o suoni raccolti siano conservati temporaneamente(11). Al di fuori di tali precisazioni, il trattamento, che venga effettuato tramite sistemi di videosorveglianza e che sia riconducibile a quanto disposto dall'art. 37 del Codice, deve essere preventivamente notificato a questa Autorità.

La mancata o incompleta notificazione ai sensi degli artt. 37 e 38 del Codice è punita con la sanzione amministrativa prevista dall'art. 163.

3.3. Misure di sicurezza da applicare ai dati personali trattati mediante sistemi di videosorveglianza e soggetti preposti

3.3.1. Misure di sicurezza

I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini (artt. 31 e ss. del Codice).

Devono quindi essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (se soggetto distinto dal titolare medesimo, nel caso in cui questo sia persona fisica).

E' inevitabile che -in considerazione dell'ampio spettro di utilizzazione di sistemi di videosorveglianza, anche in relazione ai soggetti e alle finalità perseguite nonché della varietà dei sistemi tecnologici utilizzati- le misure minime di sicurezza possano variare anche significativamente. E' tuttavia necessario che le stesse siano quanto meno rispettose dei principi che seguono:

a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini (v. punto 3.3.2). Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati incaricati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;

b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;

c) per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto (v. punto 3.4);

d) nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;

e) qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-*ter* del codice penale;

f) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie *wi-fi, wi-max, Gprs*).

3.3.2. Responsabili e incaricati

Il titolare o il responsabile devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini (*art. 30 del Codice*). Deve trattarsi di un numero delimitato di soggetti, specie quando il titolare si avvale di collaboratori esterni. Occorre altresì individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.) (v. punto 3.3.1).

Vanno osservate le regole ordinarie anche per ciò che attiene all'eventuale designazione di responsabili del trattamento (*art. 29 del Codice*).
Il mancato rispetto di quanto previsto nelle lettere da a) ad f) del punto 3.3.1 comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.
L'omessa adozione delle misure minime di sicurezza comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*bis*, ed integra la fattispecie di reato prevista dall'art. 169 del Codice.

3.4.Durata dell'eventuale conservazione

Nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità (*v. art. 11, comma 1, lett. e),del Codice*), anche l'eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario - e predeterminato - a raggiungere la finalità perseguita.
La conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Solo in alcuni casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un tempo più ampio di conservazione dei dati che, sulla scorta anche del tempo massimo legislativamente posto per altri trattamenti, si ritiene non debba comunque superare la settimana.
Per i comuni e nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, alla luce delle recenti disposizioni normative(12), il termine massimo di durata della conservazione dei dati è limitato *"ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione"*.
In tutti i casi in cui si voglia procedere a un allungamento dei tempi di conservazione per un periodo superiore alla settimana, una richiesta in tal senso deve essere sottoposta ad una verifica preliminare del Garante (v. punto 3.2.1), e comunque essere ipotizzato dal titolare come eccezionale nel rispetto del principio di proporzionalità. La congruità di un termine di tempo più ampio di conservazione va adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità. La relativa congruità può altresì dipendere dalla necessità di aderire ad una specifica richiesta di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o dalla polizia giudiziaria in relazione ad un'attività investigativa in corso.
Il sistema impiegato deve essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.
In presenza di impianti basati su tecnologia non digitale o comunque non dotati di capacità di elaborazione tali da consentire la realizzazione di meccanismi automatici di expiring dei dati registrati, la cancellazione delle immagini dovrà comunque essere effettuata nel più breve tempo possibile per l'esecuzione materiale delle operazioni dalla fine del periodo di conservazione fissato dal titolare.
Il mancato rispetto dei tempi di conservazione delle immagini raccolte e del correlato obbligo di cancellazione di dette immagini oltre il termine previsto comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.

3.5. Diritti degli interessati

Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità al Codice, in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento (*art. 7 del Codice*).

La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti al richiedente identificabile e può comprendere eventuali dati riferiti a terzi solo nei limiti previsti dal Codice, ovvero nei soli casi in cui la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato (*art. 10, comma 5, del Codice*).
In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo (*art. 7, comma 3, lett. a), del Codice*). Viceversa, l'interessato ha diritto di ottenere il blocco dei dati qualora essi siano trattati in violazione di legge (*art. 7, comma 3, lett. b), del Codice*).

4. SETTORI SPECIFICI

4.1. Rapporti di lavoro

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*). Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro: in tali casi, ai sensi dell'art. 4 della l. n. 300/1970, gli impianti e le apparecchiature, "*dai quali può derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti" (v., altresì, artt. 113 e 114 del Codice; art. 8 l. n. 300/1970 cit.; art. 2 d.lg. n. 165/2001).*
Tali garanzie vanno osservate sia all'interno degli edifici, sia in altri contesti in cui è resa la prestazione di lavoro, come, ad esempio, nei cantieri edili o con riferimento alle telecamere installate su veicoli adibiti al servizio di linea per il trasporto di persone (artt. 82, 85-87, d.lg. 30 aprile 1992, n. 285, "*Nuovo codice della strada"*) o su veicoli addetti al servizio di noleggio con conducente e servizio di piazza (taxi) per trasporto di persone (le quali non devono riprendere in modo stabile la postazione di guida, e le cui immagini, raccolte per finalità di sicurezza e di eventuale accertamento di illeciti, non possono essere utilizzate per controlli, anche indiretti, sull'attività lavorativa degli addetti, v. punto 4.4).
Il mancato rispetto di quanto sopra prescritto comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.
L'utilizzo di sistemi di videosorveglianza preordinati al controllo a distanza dei lavoratori o ad effettuare indagini sulle loro opinioni integra la fattispecie di reato prevista dall'art. 171 del Codice.
Sotto un diverso profilo, eventuali riprese televisive sui luoghi di lavoro per documentare attività od operazioni solo per scopi divulgativi o di comunicazione istituzionale o aziendale, e che vedano coinvolto il personale dipendente, possono essere assimilati ai trattamenti temporanei finalizzati alla pubblicazione occasionale di articoli, saggi ed altre manifestazioni del pensiero. In tal caso, alle stesse si applicano le disposizioni sull'attività giornalistica contenute nel Codice (*artt. 136 e ss.*), fermi restando, comunque, i limiti al diritto di cronaca posti a tutela della riservatezza, nonché l'osservanza del codice deontologico per l'attività giornalistica ed il diritto del lavoratore a tutelare la propria immagine opponendosi, per motivi legittimi, alla sua diffusione (*art. 7, comma 4, lett. a), del Codice*).

4.2. Ospedali e luoghi di cura

L'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (ad es. unità di rianimazione, reparti di isolamento), stante la natura sensibile di molti dati che possono essere in tal modo raccolti, devono essere limitati ai casi di comprovata indispensabilità, derivante da specifiche esigenze di cura e tutela della salute degli interessati.

Devono essere inoltre adottati tutti gli ulteriori accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate, anche in attuazione di quanto prescritto dal provvedimento generale del 9 novembre 2005 adottato in attuazione dell'art. 83 del Codice(13).
Il titolare deve garantire che possano accedere alle immagini rilevate per le predette finalità solo i soggetti specificamente autorizzati (es. personale medico ed infermieristico). Particolare attenzione deve essere riservata alle modalità di accesso alle riprese video da parte di terzi legittimati (familiari, parenti, conoscenti) di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (es. rianimazione), ai quali può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto o conoscente.
Le immagini idonee a rivelare lo stato di salute non devono essere comunque diffuse (*art. 22, comma 8, del Codice*). In tale quadro, va assolutamente evitato il rischio di diffusione delle immagini di persone malate su *monitor* collocati in locali liberamente accessibili al pubblico.
Il mancato rispetto di quanto sopra prescritto comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.
La diffusione di immagini in violazione dell'art. 22, comma 8, del Codice, oltre a comportare l'applicazione della sanzione amministrativa prevista dall'art. 162, comma 2-*bis*, integra la fattispecie di reato stabilita dall'art. 167, comma 2.

4.3. Istituti scolastici

L'eventuale installazione di sistemi di videosorveglianza presso istituti scolastici deve garantire *"il diritto dello studente alla riservatezza"* (*art. 2, comma 2, d.P.R. n. 249/1998*), prevedendo opportune cautele al fine di assicurare l'armonico sviluppo delle personalità dei minori in relazione alla loro vita, al loro processo di maturazione ed al loro diritto all'educazione(14).
4.3.1. In tale quadro, può risultare ammissibile l'utilizzo di tali sistemi in casi di stretta indispensabilità, al fine di tutelare l'edificio ed i beni scolastici da atti vandalici, circoscrivendo le riprese alle sole aree interessate ed attivando gli impianti negli orari di chiusura degli istituti; è vietato, altresì, attivare le telecamere in coincidenza con lo svolgimento di eventuali attività extrascolastiche che si svolgono all'interno della scuola.
4.3.2. Laddove la ripresa delle immagini riguardi anche le aree perimetrali esterne degli edifici scolastici, l'angolo visuale deve essere delimitato alle sole parti interessate, escludendo dalle riprese le aree non strettamente pertinenti l'edificio.
4.3.3. Il mancato rispetto di quanto prescritto ai punti 4.3.1 e 4.3.2 comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-ter, del Codice.

4.4. Sicurezza nel trasporto pubblico

4.4.1. Alcune situazioni di particolare rischio possono fare ritenere lecita l'installazione di sistemi di videosorveglianza sia su mezzi di trasporto pubblici, sia presso le fermate dei predetti mezzi.
4.4.2. La localizzazione delle telecamere e le modalità di ripresa devono essere determinate nel rispetto dei richiamati principi di necessità, proporzionalità e finalità; pertanto, occorre evitare riprese particolareggiate nei casi in cui le stesse non sono indispensabili in relazione alle finalità perseguite.
4.4.3. I titolari del trattamento dovranno poi provvedere a fornire la prevista informativa agli utenti del servizio di trasporto urbano. Gli autobus, i tram, i taxi ed i veicoli da noleggio con o senza conducente dotati di telecamere dovranno pertanto portare apposite indicazioni o contrassegni che diano conto con immediatezza della presenza dell'impianto di videosorveglianza, anche utilizzando a tal fine il *fac-simile* riportato nell'allegato n. 1 al presente provvedimento, e indicanti, comunque, il titolare del trattamento, nonché la finalità perseguita.
4.4.4. Specifiche cautele devono essere osservate laddove vengano installati impianti di videosorveglianza presso le aree di fermata, in prossimità delle quali possono transitare anche soggetti diversi dagli utenti del servizio di trasporto pubblico. In particolare, l'angolo visuale delle apparecchiature di ripresa deve essere strettamente circoscritto all'area di permanenza, permettendo l'inquadratura solo della pensilina e di altri arredi urbani funzionali al servizio di trasporto pubblico

(tabelle degli orari, paline recanti l'indicazione degli autobus in transito, ecc.), con esclusione della zona non immediatamente circostante e comunque dell'area non direttamente funzionale rispetto alle esigenze di sicurezza del sistema di traffico e trasporto. Anche in tale ipotesi occorre evitare le riprese inutilmente particolareggiate o tali da rilevare caratteristiche eccessivamente dettagliate degli individui che stazionano presso le fermate. L'esistenza delle telecamere deve essere opportunamente evidenziata nelle predette aree di fermata.

4.4.5. Fermo restando che la violazione delle disposizioni riguardanti l'informativa di cui all'art. 13 è punita con la sanzione amministrativa prevista dall'art. 161 del Codice e l'utilizzo di sistemi di videosorveglianza preordinati al controllo a distanza dei lavoratori integra la fattispecie di reato prevista dall'art. 171, il mancato rispetto di quanto prescritto al punto 4.4.4 comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.

4.5. Utilizzo di web cam o camera-on-line a scopi promozionali-turistici o pubblicitari

Le attività di rilevazione di immagini a fini promozionali-turistici o pubblicitari, attraverso *web cam* devono avvenire con modalità che rendano non identificabili i soggetti ripresi. Ciò in considerazione delle peculiari modalità del trattamento, dalle quali deriva un concreto rischio del verificarsi di un pregiudizio rilevante per gli interessati: le immagini raccolte tramite tali sistemi, infatti, vengono inserite direttamente sulla rete Internet, consentendo a chiunque navighi sul web di visualizzare in tempo reale i soggetti ripresi e di utilizzare le medesime immagini anche per scopi diversi dalle predette finalità promozionali-turistiche o pubblicitarie perseguite dal titolare del trattamento.

4.6. Sistemi integrati di videosorveglianza

In ottemperanza del principio di economicità delle risorse e dei mezzi impiegati, si è incrementato il ricorso a sistemi integrati di videosorveglianza tra diversi soggetti, pubblici e privati, nonché l'offerta di servizi centralizzati di videosorveglianza remota da parte di fornitori (società di vigilanza, *Internet service providers*, fornitori di servizi video specialistici, ecc.). Inoltre, le immagini riprese vengono talvolta rese disponibili, con varie tecnologie o modalità, alle forze di polizia.

Nell'ambito dei predetti trattamenti, sono individuabili le seguenti tipologie di sistemi integrati di videosorveglianza:

a) *gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, delle immagini riprese da parte di diversi e autonomi titolari del trattamento*, i quali utilizzano le medesime infrastrutture tecnologiche; in tale ipotesi, i singoli titolari possono trattare le immagini solo nei termini strettamente funzionali al perseguimento dei propri compiti istituzionali ed alle finalità chiaramente indicate nell'informativa, nel caso dei soggetti pubblici, ovvero alle sole finalità riportate nell'informativa, nel caso dei soggetti privati;

b) *collegamento telematico di diversi titolari del trattamento ad un "centro" unico gestito da un soggetto terzo*; tale soggetto terzo, designato responsabile del trattamento ai sensi dell'art. 29 del Codice da parte di ogni singolo titolare, deve assumere un ruolo di coordinamento e gestione dell'attività di videosorveglianza senza consentire, tuttavia, forme di correlazione delle immagini raccolte per conto di ciascun titolare;

c) sia nelle predette ipotesi, sia nei casi in cui l'attività di videosorveglianza venga effettuata da un solo titolare, si può anche attivare un *collegamento dei sistemi di videosorveglianza con le sale o le centrali operative degli organi di polizia*. L'attivazione del predetto collegamento deve essere reso noto agli interessati. A tal fine, il Garante ritiene che si possa utilizzare il modello semplificato di informativa "minima" - indicante il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia- individuato ai sensi dell'art. 13, comma 3, del Codice e riportato in *fac-simile* nell'allegato n. 2 al presente provvedimento. Tale collegamento deve essere altresì reso noto nell'ambito del testo completo di informativa reso eventualmente disponibile agli interessati (v. punto 3.1.3).

Le modalità di trattamento sopra elencate richiedono l'adozione di specifiche misure di sicurezza ulteriori rispetto a quelle individuate nel precedente punto 3.3.1, quali:

1) adozione di sistemi idonei alla registrazione degli accessi logici degli incaricati e delle operazioni compiute sulle immagini registrate, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato dei responsabili da parte del titolare, comunque non inferiore a sei mesi;
2) separazione logica delle immagini registrate dai diversi titolari.
Il mancato rispetto delle misure previste ai punti 1) e 2) comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.
Fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere una verifica preliminare a questa Autorità (v. punto 3.2.1).

5. SOGGETTI PUBBLICI

I soggetti pubblici, in qualità di titolari del trattamento (*art. 4, comma 1, lett. f), del Codice*), possono trattare dati personali nel rispetto del principio di finalità, perseguendo scopi determinati, espliciti e legittimi (*art. 11, comma 1, lett. b), del Codice*), soltanto per lo svolgimento delle proprie funzioni istituzionali. Ciò vale ovviamente anche in relazione a rilevazioni di immagini mediante sistemi di videosorveglianza (*art. 18, comma 2, del Codice*).
I soggetti pubblici sono tenuti a rispettare, al pari di ogni titolare di trattamento effettuato tramite sistemi di videosorveglianza, i principi enunciati nel presente provvedimento.
Anche per i soggetti pubblici sussiste l'obbligo di fornire previamente l'informativa agli interessati (*art. 13 del Codice*), ferme restando le ipotesi prese in considerazione al punto 3.1.1. Pertanto, coloro che accedono o transitano in luoghi dove sono attivi sistemi di videosorveglianza devono essere previamente informati in ordine al trattamento dei dati personali. A tal fine, anche i soggetti pubblici possono utilizzare il modello semplificato di informativa "minima", riportato in *fac-simile* nell'allegato n. 1 al presente provvedimento (v. punto 3.1).

5.1. Sicurezza urbana

Recenti disposizioni legislative in materia di sicurezza hanno attribuito ai sindaci il compito di sovrintendere alla vigilanza ed all'adozione di atti che sono loro attribuiti dalla legge e dai regolamenti in materia di ordine e sicurezza pubblica, nonché allo svolgimento delle funzioni affidati ad essi dalla legge in materia di sicurezza e di polizia giudiziaria(15). Al fine di prevenire e contrastare determinati pericoli(16) che minacciano l'incolumità pubblica e la sicurezza urbana, il sindaco può altresì adottare provvedimenti, anche contingibili e urgenti, nel rispetto dei principi generali dell'ordinamento. Infine, il sindaco, quale ufficiale del Governo, concorre ad assicurare la cooperazione della polizia locale con le forze di polizia statali, nell'ambito delle direttive di coordinamento impartite dal Ministero dell'interno.
Da tale quadro emerge che sussistono specifiche funzioni attribuite sia al sindaco, quale ufficiale del Governo, sia ai comuni, rispetto alle quali i medesimi soggetti possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico al fine di tutelare la sicurezza urbana(17).
Non spetta a questa Autorità definire il concetto di sicurezza urbana e delimitarne l'ambito operativo rispetto a quelli di ordine e sicurezza pubblica; purtuttavia, resta inteso che, nelle ipotesi in cui le attività di videosorveglianza siano assimilabili alla tutela della sicurezza pubblica, nonché alla prevenzione, accertamento o repressione dei reati, trova applicazione l'art. 53 del Codice (v. punto 3.1.1).
In ogni caso, si ribadisce l'auspicio che, nelle predette ipotesi, l'informativa, benché non obbligatoria, venga comunque resa, specie laddove i comuni ritengano opportuno rendere noto alla cittadinanza l'adozione di misure e accorgimenti, quali l'installazione di sistemi di videosorveglianza, volti al controllo del territorio e alla protezione degli individui.

5.2. Deposito dei rifiuti

In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza risulta lecito con riferimento alle attività di controllo volte ad accertare l'utilizzo

abusivo di aree impiegate come discariche di materiali e di sostanze pericolose solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi.
Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (art. 13, l. 24 novembre 1981, n. 689).

5.3. Utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della strada

Gli impianti elettronici di rilevamento automatizzato delle infrazioni, utilizzati per documentare la violazione delle disposizioni in materia di circolazione stradale, analogamente all'utilizzo di sistemi di videosorveglianza, comportano un trattamento di dati personali.
5.3.1. L'utilizzo di tali sistemi è quindi lecito se sono raccolti solo dati pertinenti e non eccedenti per il perseguimento delle finalità istituzionali del titolare, delimitando a tal fine la dislocazione e l'angolo visuale delle riprese in modo da non raccogliere immagini non pertinenti o inutilmente dettagliate. In conformità alla prassi ed al quadro normativo di settore riguardante talune violazioni del Codice della strada(18), il Garante prescrive quanto segue:
a) gli impianti elettronici di rilevamento devono circoscrivere la conservazione dei dati alfanumerici contenuti nelle targhe automobilistiche ai soli casi in cui risultino non rispettate le disposizioni in materia di circolazione stradale;
b) le risultanze fotografiche o le riprese video possono individuare unicamente gli elementi previsti dalla normativa di settore per la predisposizione del verbale di accertamento delle violazioni (*es., ai sensi dell'art. 383 del d.P.R. n. 495/1992, il tipo di veicolo, il giorno, l'ora e il luogo nei quali la violazione è avvenuta*); deve essere effettuata una ripresa del veicolo che non comprenda o, in via subordinata, mascheri, per quanto possibile, la porzione delle risultanze video/fotografiche riguardanti soggetti non coinvolti nell'accertamento amministrativo (es., pedoni, altri utenti della strada);
c) le risultanze fotografiche o le riprese video rilevate devono essere utilizzate solo per accertare le violazioni delle disposizioni in materia di circolazione stradale anche in fase di contestazione, ferma restando la loro accessibilità da parte degli aventi diritto;
d) le immagini devono essere conservate per il periodo di tempo strettamente necessario in riferimento alla contestazione, all'eventuale applicazione di una sanzione e alla definizione del possibile contenzioso in conformità alla normativa di settore(19), fatte salve eventuali esigenze di ulteriore conservazione derivanti da una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria;
e) le fotografie o le immagini che costituiscono fonte di prova per le violazioni contestate non devono essere inviate d'ufficio al domicilio dell'intestatario del veicolo unitamente al verbale di contestazione, ferma restando la loro accessibilità agli aventi diritto;
f) in considerazione del legittimo interesse dell'intestatario del veicolo di verificare l'autore della violazione e, pertanto, di ottenere dalla competente autorità ogni elemento a tal fine utile, la visione della documentazione video-fotografica deve essere resa disponibile a richiesta del destinatario del verbale; al momento dell'accesso, dovranno essere opportunamente oscurati o resi comunque non riconoscibili i passeggeri presenti a bordo del veicolo.
Il mancato rispetto di quanto sopra prescritto nelle lettere da a) ad f) comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-ter, del Codice.
5.3.2. Anche i conducenti dei veicoli e le persone che accedono o transitano in aree dove sono attivi sistemi elettronici di rilevazione automatizzata delle violazioni devono essere previamente informati in ordine al trattamento dei dati personali (*art. 13 del Codice*).
Particolari disposizioni normative vigenti individuano già talune ipotesi (come, ad es., in caso di rilevamento a distanza dei limiti di velocità) in cui l'amministrazione pubblica è tenuta a informare gli utenti in modo specifico in ordine all'utilizzo di dispositivi elettronici(20).
L'obiettivo da assicurare è quello di un'efficace informativa agli interessati, che può essere fornita dagli enti preposti alla rilevazione delle immagini attraverso più soluzioni.

Un'idonea informativa in materia può essere anzitutto assicurata mediante l'utilizzo di strumenti appropriati che rendano agevolmente conoscibile l'esistenza e la presenza nelle aree interessate degli strumenti di rilevamento di immagini. A tal fine, svolgono un ruolo efficace gli strumenti di comunicazione al pubblico e le iniziative periodiche di diffusa informazione (*siti web*, comunicati scritti); tali forme di informazione possono essere eventualmente integrate con altre modalità (es., volantini consegnati all'utenza, pannelli a messaggio variabile, annunci televisivi e radiofonici, reti civiche e altra comunicazione istituzionale).
A integrazione di tali strumenti di comunicazione e informazione, va considerato il contributo che possono dare appositi cartelli. A tal fine, il modello semplificato di informativa "minima", riportato nel *fac-simile* in allegato, può essere utilizzato nei casi in cui la normativa in materia di circolazione stradale non prevede espressamente l'obbligo di informare gli utenti relativamente alla presenza di dispositivi elettronici volti a rilevare automaticamente le infrazioni.
Come si è detto, la normativa di settore prevede espressamente, in alcuni casi (es., rilevamento a distanza dei limiti di velocità, dei sorpassi vietati), l'obbligo di rendere nota agli utenti l'installazione degli impianti elettronici di rilevamento automatizzato delle infrazioni. In questi stessi casi è quindi possibile fare a meno di fornire un'ulteriore, distinta informativa rispetto al trattamento dei dati che riproduca gli elementi che sono già noti agli interessati per effetto degli avvisi di cui alla disciplina di settore in tema di circolazione stradale (*art. 13, comma 2, del Codice*). L'installazione di questi ultimi appositi avvisi previsti dal Codice della strada permette già agli interessati di percepire vari elementi essenziali in ordine al trattamento dei propri dati personali. Pertanto, gli avvisi che segnalano adeguatamente l'attivazione di dispositivi elettronici di rilevazione automatica delle infrazioni possono essere considerati idonei ad adempiere all'obbligo di fornire l'informativa di cui all'art. 13 del Codice.
Infine, l'obbligo di fornire tale informativa deve ritenersi soddisfatto anche quando il titolare del trattamento, pur mancando una previsione normativa che obblighi specificamente a segnalare la rilevazione automatizzata, la segnali comunque utilizzando avvisi analoghi a quelli previsti dal Codice della strada.
La violazione delle disposizioni riguardanti l'informativa di cui all'art. 13 è punita con la sanzione amministrativa prevista dall'art. 161 del Codice.
5.3.3. Qualora si introducano sistemi di rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato, i comuni dovranno rispettare quanto previsto dal d.P.R. 22 giugno 1999, n. 250. Tale normativa prevede che i dati trattati possono essere conservati solo per il periodo necessario per contestare le infrazioni e definire il relativo contenzioso, ferma restando l'accessibilità agli stessi per fini di polizia giudiziaria o di indagine penale (*art. 3 d.P.R. n. 250/1999*).

5.4. Ulteriori avvertenze per i sistemi di videosorveglianza posti in essere da enti pubblici e, in particolare, da enti territoriali

Anche gli enti territoriali e, in generale, i soggetti pubblici operanti sul territorio effettuano attività di videosorveglianza in forma integrata, tramite la compartecipazione ad un medesimo sistema di rilevazione, al fine di economizzare risorse e mezzi impiegati nell'espletamento delle più diverse attività istituzionali.
Questa Autorità ha già individuato al punto 4.6 un quadro di specifiche garanzie in ordine alle corrette modalità che vengono qui ulteriormente richiamate, in particolare con riferimento all'attività del controllo sul territorio da parte dei comuni, anche relativamente a quanto disposto in materia di videosorveglianza comunale(21).
In particolare:
a) l'utilizzo condiviso, in forma integrale o parziale, di sistemi di videosorveglianza tramite la medesima infrastruttura tecnologica deve essere configurato con modalità tali da permettere ad ogni singolo ente e, in taluni casi, anche alle diverse strutture organizzative dell'ente, l'accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti istituzionali,

evitando di tracciare gli spostamenti degli interessati e di ricostruirne il percorso effettuato in aree che esulano dalla competenza territoriale dell'ente;
b) nei casi in cui un "centro" unico gestisca l'attività di videosorveglianza per conto di diversi soggetti pubblici, i dati personali raccolti dovranno essere trattati in forma differenziata e rigorosamente distinta, in relazione alle competenze istituzionali della singola pubblica amministrazione.
Il titolare del trattamento è tenuto a richiedere una verifica preliminare a questa Autorità fuori dalle predette ipotesi, ed in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento, agli effetti che possono determinare o, a maggior ragione, con riferimento a quei sistemi per i quali già il punto 3.2.1 la richiede (es. sistemi di raccolta delle immagini associate a dati biometrici o c.d. intelligenti, cioè in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli).

6. PRIVATI ED ENTI PUBBLICI ECONOMICI

6.1. Trattamento di dati personali per fini esclusivamente personali

L'installazione di sistemi di videosorveglianza -come si rileva dall'esame di numerose istanze pervenute all'Autorità- viene sovente effettuata da persone fisiche per fini esclusivamente personali. In tal caso va chiarito che la disciplina del Codice non trova applicazione qualora i dati non siano comunicati sistematicamente a terzi ovvero diffusi, risultando comunque necessaria l'adozione di cautele a tutela dei terzi (*art. 5, comma 3*, del Codice, che fa salve le disposizioni in tema di responsabilità civile e di sicurezza dei dati). In tali ipotesi possono rientrare, a titolo esemplificativo, strumenti di videosorveglianza idonei ad identificare coloro che si accingono ad entrare in luoghi privati (videocitofoni ovvero altre apparecchiature che rilevano immagini o suoni, anche tramite registrazione), oltre a sistemi di ripresa installati nei pressi di immobili privati ed all'interno di condomini e loro pertinenze (quali posti auto e *box*).
Benché non trovi applicazione la disciplina del Codice, al fine di evitare di incorrere nel reato di interferenze illecite nella vita privata (*art. 615-bis c.p.*), l'angolo visuale delle riprese deve essere comunque limitato ai soli spazi di propria esclusiva pertinenza (ad esempio antistanti l'accesso alla propria abitazione) escludendo ogni forma di ripresa, anche senza registrazione di immagini, relativa ad aree comuni (cortili, pianerottoli, scale, garage comuni) ovvero ad ambiti antistanti l'abitazione di altri condomini.

6.2. Trattamento di dati personali per fini diversi da quelli esclusivamente personali

6.2.1. Consenso

Nel caso in cui trovi applicazione la disciplina del Codice, il trattamento di dati può essere lecitamente effettuato da privati ed enti pubblici economici solamente se vi sia il consenso preventivo dell'interessato, oppure se ricorra uno dei presupposti di liceità previsti in alternativa al consenso (*artt. 23 e 24 del Codice*).
Nel caso di impiego di strumenti di videosorveglianza la possibilità di acquisire il consenso risulta in concreto limitata dalle caratteristiche stesse dei sistemi di rilevazione che rendono pertanto necessario individuare un'idonea alternativa nell'ambito dei requisiti equipollenti del consenso di cui all'art. 24, comma 1, del Codice.

6.2.2. Bilanciamento degli interessi

Tale alternativa può essere ravvisata nell'istituto del bilanciamento di interessi (*art. 24, comma 1, lett. g), del Codice*). Il presente provvedimento dà attuazione a tale istituto, individuando i casi in cui la rilevazione delle immagini può avvenire senza consenso, qualora, con le modalità stabilite in questo stesso provvedimento, sia effettuata nell'intento di perseguire un legittimo interesse del titolare o di un terzo attraverso la raccolta di mezzi di prova o perseguendo fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, o finalità di prevenzione di incendi o di sicurezza del lavoro.

A tal fine, possono essere individuati i seguenti casi, in relazione ai quali, con le precisazioni di seguito previste, il trattamento può lecitamente avvenire pure in assenza del consenso.

6.2.2.1. Videosorveglianza (con o senza registrazione delle immagini)

Tali trattamenti sono ammessi in presenza di concrete situazioni che giustificano l'installazione, a protezione delle persone, della proprietà o del patrimonio aziendale.

Nell'uso delle apparecchiature volte a riprendere, con o senza registrazione delle immagini, aree esterne ad edifici e immobili (perimetrali, adibite a parcheggi o a carico/scarico merci, accessi, uscite di emergenza), resta fermo che il trattamento debba essere effettuato con modalità tali da limitare l'angolo visuale all'area effettivamente da proteggere, evitando, per quanto possibile, la ripresa di luoghi circostanti e di particolari che non risultino rilevanti (vie, edifici, esercizi commerciali, istituzioni ecc.).

6.2.2.2. Riprese nelle aree condominiali comuni

Qualora i trattamenti siano effettuati dal condominio (anche per il tramite della relativa amministrazione), si evidenzia che tale specifica ipotesi è stata recentemente oggetto di una segnalazione da parte del Garante al Governo ed al Parlamento(22); ciò in relazione all'assenza di una puntuale disciplina che permetta di risolvere alcuni problemi applicativi evidenziati nell'esperienza di questi ultimi anni. Non è infatti chiaro se l'installazione di sistemi di videosorveglianza possa essere effettuata in base alla sola volontà dei comproprietari, o se rilevi anche la qualità di conduttori. Non è parimenti chiaro quale sia il numero di voti necessario per la deliberazione condominiale in materia (se occorra cioè l'unanimità ovvero una determinata maggioranza).

7. PRESCRIZIONI E SANZIONI

Il Garante invita tutti i titolari dei trattamenti di dati personali effettuati tramite sistemi di videosorveglianza ad attenersi alle prescrizioni indicate nel presente provvedimento.

Le misure necessarie prescritte con il presente provvedimento devono essere osservate da tutti i titolari di trattamento. In caso contrario il trattamento dei dati è, a seconda dei casi, illecito oppure non corretto, ed espone:

• all'inutilizzabilità dei dati personali trattati in violazione della relativa disciplina (*art. 11, comma 2, del Codice*);

• all'adozione di provvedimenti di blocco o di divieto del trattamento disposti dal Garante (*art. 143, comma 1, lett. c*), del Codice), e di analoghe decisioni adottate dall'autorità giudiziaria civile e penale;

• all'applicazione delle pertinenti sanzioni amministrative o penali (*artt. 161 e ss. del Codice*).

TUTTO CIÒ PREMESSO IL GARANTE:

1. prescrive ai sensi dell'art. 154, comma 1, lett. c), del Codice, ai titolari del trattamento di dati personali effettuato tramite sistemi di videosorveglianza, di adottare al più presto e, comunque, entro e non oltre i distinti termini di volta in volta indicati decorrenti dalla data di pubblicazione del presente provvedimento nella Gazzetta Ufficiale della Repubblica italiana, le misure e gli accorgimenti illustrati in premessa e di seguito individuati concernenti l'obbligo di:

a) entro dodici mesi, rendere l'informativa visibile anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno (punto 3.1);

b) entro sei mesi, sottoporre i trattamenti che presentano rischi specifici per i diritti e le libertà fondamentali degli interessati, alla verifica preliminare ai sensi dell'art. 17 del Codice (punto 3.2.1);

c) entro dodici mesi, adottare, le misure di sicurezza a protezione dei dati registrati tramite impianti di videosorveglianza (punto 3.3);

d) entro sei mesi, adottare le misure necessarie per garantire il rispetto di quanto indicato nei punti 4.6 e 5.4, per quanto concerne i sistemi integrati di videosorveglianza;

2. individua, nei termini di cui in motivazione, ai sensi dell'art. 24, comma 1, lett. *g*), del Codice, i casi nei quali il trattamento dei dati personali mediante videosorveglianza può essere effettuato da soggetti privati ed enti pubblici economici, nei limiti e alle condizioni indicate, per perseguire legittimi interessi e senza richiedere il consenso degli interessati (punto 6.2.2);

3. individua nell'allegato 1, ai sensi dell'art. 13, comma 3, del Codice, un modello semplificato di informativa utilizzabile alle condizioni indicate in motivazione (punto 3.1);
4. individua nell'allegato 2, ai sensi dell'art. 13, comma 3, del Codice, un modello semplificato di informativa utilizzabile alle condizioni indicate in motivazione, al fine di rendere noto agli interessati l'attivazione di un collegamento del sistema di videosorveglianza con le forze di polizia (punti 3.1.3 e 4.6, lett. c));
5. segnala l'opportunità che, anche nell'espletamento delle attività di cui all'art. 53 del Codice, l'informativa, benché non obbligatoria, sia comunque resa in tutti i casi nei quali non ostano in concreto specifiche ragioni di tutela e sicurezza pubblica o di prevenzione, accertamento o repressione dei reati (punto 5.1);
6. dispone, ai sensi dell'art. 143, comma 2, del Codice, che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti per la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana.
Roma, 8 aprile 2010

IL PRESIDENTE
F.to Pizzetti

IL RELATORE
F.to Pizzetti

IL SEGRETARIO GENERALE REGGENTE
F.to De Paoli

NOTE
(1). In *www.garanteprivacy.it*; doc. web n. 1003482.
(2). V. l'art. 6, comma 8, del d.l. 23 febbraio 2009, n. 11 convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 23 aprile 2009, n. 38, recante *"Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori"*; d.l. 23 maggio 2008, n. 92, convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 24 luglio 2008, n. 125, recante *"Misure urgenti in materia di sicurezza urbana"*, il cui art. 6 ha novellato l'art. 54 del d.lg. 18 agosto 2000, n. 267, con cui sono stati disciplinati i compiti del sindaco in materia di ordine e sicurezza pubblica. Con il decreto del 5 agosto 2008 il Ministro dell'interno ha stabilito l'ambito di applicazione, individuando la definizione di incolumità pubblica e sicurezza urbana, nonché i correlati ambiti di intervento attribuiti al sindaco. Cfr., altresì, l. 15 luglio 2009, n. 94 recante *"Disposizioni in materia di sicurezza pubblica"* (art. 3).
(3). A tale proposito, va ricordata la l. 24 dicembre 2007, n. 244 recante *"Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2008)"*, il cui art. 1, comma 228, ha previsto, ai fini dell'adozione di misure finalizzate a prevenire il rischio del compimento di atti illeciti da parte di terzi, compresa l'installazione di apparecchi di videosorveglianza, per ciascuno dei periodi d'imposta 2008, 2009 e 2010, la concessione da parte dell'Agenzia delle entrate (*v. d.m. 6 febbraio 2008* recante *"Modalità di attuazione dei commi da 233 a 237, dell'articolo 1, della legge n. 244/2007- credito d'imposta in favore degli esercenti attività di rivendita di generi di monopolio, per le spese sostenute per l'acquisizione e l'installazione di impianti e attrezzature di sicurezza e per favorire la diffusione degli strumenti di pagamento con moneta elettronica, al fine di prevenire il compimento di atti illeciti ai loro danni"*) di un credito d'imposta, determinato nella misura dell'80% del costo sostenuto e, comunque, fino ad un importo massimo di 3.000 euro per ciascun beneficiario, in favore delle piccole e medie imprese commerciali di vendita al dettaglio e all'ingrosso e quelle di somministrazione di alimenti e bevande.

(4). V., a titolo esemplificativo, l.r. Emilia Romagna, 4 dicembre 2003, n. 24 recante "Disciplina della polizia amministrativa locale e promozione di un sistema integrato di sicurezza"; l.r. Friuli Venezia Giulia, 28 dicembre 2007, n. 30 recante "Legge strumentale alla manovra di bilancio (Legge strumentale 2008)"; l.r. Lombardia, 14 aprile 2003, n. 4, recante *"Riordino e riforma della disciplina regionale in materia di polizia locale e sicurezza urbana"*; la l.r. Sicilia, 3 dicembre 2003, n. 20 recante *"Norme finanziarie urgenti e variazioni al bilancio della Regione per l'anno finanziario 2003. Norme di razionalizzazione in materia di organizzazione amministrativa e di sviluppo economico"*.
(5). V., in particolare l'art. 615-bis del codice penale. V. *Provv*. 2 ottobre 2008, doc. *web* n. 1581352.
(6). L. 20 maggio 1970, n. 300
(7). D.l. 24 febbraio 2003, n. 28, convertito, con modificazioni, con l. 24 aprile 2003, n. 88; v. *parere* reso al Ministero dell'interno del 4 maggio 2005, doc. *web* n. 1120732.
(8). D.l. 14 novembre 1992, n. 433, convertito, con modificazioni, dalla legge 14 gennaio 1993, n. 4.
(9). D.lg. 4 febbraio 2000, n. 45.
(10). D.m. 15 settembre 2009 n. 154, recante *"Regolamento recante disposizioni per l'affidamento dei servizi di sicurezza sussidiaria nell'ambito dei porti, delle stazioni ferroviarie e dei relativi mezzi di trasporto e depositi, delle stazioni delle ferrovie metropolitane e dei relativi mezzi di trasporto e depositi, nonché nell'ambito delle linee di trasporto urbano, per il cui espletamento non è richiesto l'esercizio di pubbliche potestà, adottato ai sensi dell'articolo 18, comma 2, del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155"*.
(11). *Provv*. 31 marzo 2004, n. 1/2004 relativo ai casi da sottrarre all'obbligo di notificazione (pubblicato in G.U. 6 aprile 2004, n. 81; doc. *web* n. 852561); v. anche i chiarimenti forniti con nota n. 9654/33365 del 23 aprile 2004 relativamente alla posizione geografica delle persone, doc. *web* n. 993385.
(12). Così stabilito dall'art. 6, comma 8, del d.l. n. 11/2009 cit.
(13). *Provv*. 9 novembre 2005, doc. *web* n. 1191411.
(14). *Provv*. 4 settembre 2009, doc. *web* n. 1651744.
(15). D.l. n. 92/2008 cit.
(16). D.m. 5 agosto 2008 cit.
(17). V. artt. 6 d.l. n. 92/2008 cit., e 6, comma 7, d.l. n. 11/2009 cit.
(18). V. quanto previsto con riferimento al rilevamento a distanza dei limiti di velocità e dei sorpassi vietati dal d.P.R. 16 dicembre 1992, n. 495 recante *"Regolamento di esecuzione e di attuazione del nuovo codice della strada"* (art. 383); circ. Ministero dell'interno del 14 agosto 2009, n. 300/A/10307/09/144/5/20/3 recante *"Direttiva per garantire un'azione coordinata di prevenzione e contrasto dell'eccesso di velocità sulle strade"*; circ. Ministero dell'interno, Dipartimento della pubblica sicurezza, Direzione centrale per la polizia stradale, ferroviaria, delle comunicazioni e per i reparti speciali della Polizia di Stato, del 16 maggio 2008, n. 300/A/1/34197/101/138 riguardante *"Accesso ai documenti amministrativi riguardanti l'attività di accertamento e contestazione delle violazioni in materia di limiti di velocità"* (par. 6); nota del Ministero dell'interno, Dipartimento della pubblica sicurezza, Direzione centrale per la polizia stradale, ferroviaria e delle comunicazioni e per i reparti speciali della Polizia di Stato, prot. n. 300/A/1/38001/144/16/20 del 27 ottobre 2008.
(19). V., ad es., art. 3 d.P.R. 22 giugno 1999, n. 250 recante *"Regolamento recante norme per l'autorizzazione alla installazione e all'esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato, a norma dell'articolo 7, comma 133-bis, della L. 15 maggio 1997, n. 127"*.
(20). La disciplina in tema di circolazione stradale prevede che le postazioni di controllo sulla rete stradale per rilevare la velocità debbano essere segnalate preventivamente e rese ben visibili in casi specificatamente delimitati: v., ad es., quanto stabilito in ordine all'utilizzazione dei dispositivi e dei mezzi tecnici di controllo della viabilità finalizzati al rilevamento a distanza dei limiti di velocità,

dei sorpassi vietati e delle norme di comportamento sulle autostrade e sulle strade extraurbane principali (artt. 142, 148 e 176 d.lg. 30 aprile 1992, n. 285; art. 4, comma 1, d.lg. 20 giugno 2002, n. 121, conv., con mod., dall'art. 1 l. 1° agosto 2002, n. 168 recante *"Disposizioni urgenti per garantire la sicurezza nella circolazione stradale"*; d.m. 15 agosto 2007 recante *"Attuazione dell'articolo 3, comma 1, lettera b) d.l. 3 agosto 2007, n. 117, recante disposizioni urgenti modificative del codice della strada per incrementare i livelli di sicurezza nella circolazione"*; art. 7 circ. Ministero dell'interno del 14 agosto 2009, n. 300/A/10307/09/144/5/20/3 cit.; circ. Ministero dell'interno 8 aprile 2003, n. 300/A/1/41198/101/3/3/9 *"Direttive per l'utilizzazione e l'installazione dei dispositivi e dei mezzi tecnici di controllo del traffico finalizzati al rilevamento a distanza delle violazioni delle norme di comportamento di cui agli articoli 142 e 148 del d.lg. 30 aprile 1992, n. 285"*).
(21).V. art. 6, comma 8, del d.l. n. 11/2009 cit.
(22). V. segnalazione del Garante del 13 maggio 2008, doc. web n. 1523997

2.3. Linee-guida per il trattamento di dati dei dipendenti privati - 23 novembre 2006

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;
VISTO il d.lg. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), con particolare riferimento all'art. 154, comma 1, lett. h);
ESAMINATE le istanze (segnalazioni, reclami e quesiti) di lavoratori, organizzazioni sindacali ed imprese, pervenute in materia di trattamento di dati personali di lavoratori operanti alle dipendenze di datori di lavoro privati;
VISTE le pronunce adottate dall'Autorità in ordine a specifiche operazioni di trattamento di dati personali effettuate nell'ambito della gestione del rapporto di lavoro, anche a seguito di ricorso degli interessati;
RITENUTA l'opportunità di procedere alla definizione, in tale contesto, di un quadro unitario di misure ed accorgimenti necessari e opportuni in grado di fornire ulteriori orientamenti utili per i datori di lavoro e i lavoratori in ordine alle operazioni di trattamento di dati personali connesse alla gestione del rapporto di lavoro, individuando, a tal fine, i comportamenti più appropriati da adottare;
RILEVATA l'esigenza che tale quadro sia riassunto in alcune linee guida, suscettibili di periodico aggiornamento, di cui verrà curata la più ampia pubblicità, anche attraverso il sito Internet dell'Autorità ();
RITENUTA la necessità che le misure e gli accorgimenti relativi al trattamento di dati biometrici di cui al punto 4 delle Linee guida di cui al successivo dispositivo siano altresì oggetto di una prescrizione del Garante ai sensi degli artt. 17, 154, comma 1, lett. c) e 167, comma 2 del Codice, considerati i maggiori rischi specifici che tale trattamento pone per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato;
VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;
RELATORE il dott. Mauro Paissan;

DELIBERA

1. di adottare le "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati", di cui al documento che è allegato quale parte integrante della presente deliberazione (Allegato 1);
2. di prescrivere ai titolari del trattamento interessati l'adozione delle misure e degli accorgimenti per il trattamento di dati biometrici di cui al punto 4 delle medesime Linee guida, ai sensi degli artt. 17, 154, comma 1, lett. c) e 167, comma 2, del Codice;
3. che copia del presente provvedimento, unitamente alle menzionate "Linee guida", sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana ai sensi dell'art. 143, comma 2, del Codice.

Roma, 23 novembre 2006

IL PRESIDENTE
Pizzetti
IL RELATORE
Paissan
IL SEGRETARIO GENERALE
Buttarelli

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati

(Deliberazione n. 53 del 23 novembre 2006)

SOMMARIO

1. Premessa

1.1. Scopo delle linee guida. Per fornire indicazioni e raccomandazioni con riguardo alle operazioni di trattamento effettuate con dati personali (anche sensibili) di lavoratori operanti alle dipendenze di datori di lavoro privati il Garante ravvisa l'esigenza di adottare le presenti linee guida, suscettibili di periodico aggiornamento, nelle quali si tiene conto, altresì, di precedenti decisioni dell'Autorità.

Le indicazioni fornite non pregiudicano l'applicazione delle disposizioni di legge o di regolamento che stabiliscono divieti o limiti più restrittivi in relazione a taluni settori o a specifici casi di

trattamento di dati (artt. 113, 114 e 184, comma 3, del Codice) [1].

1.2. Ambiti considerati. Le tematiche prese in considerazione si riferiscono prevalentemente alla comunicazione e alla diffusione dei dati, all'informativa che il datore di lavoro deve rendere ai lavoratori (art. 13 del Codice), ai dati idonei a rivelare lo stato di salute e il diritto d'accesso.
Le operazioni di trattamento riguardano per lo più:

- dati anagrafici di lavoratori (assunti o cessati dal servizio), dati biometrici, fotografie e dati sensibili riferiti anche a terzi, idonei in particolare a rivelare il credo religioso o l'adesione a sindacati; dati idonei a rivelare lo stato di salute, di regola contenuti in certificati medici o in altra documentazione prodotta per giustificare le assenze dal lavoro o per fruire di particolari permessi e benefici previsti anche nei contratti collettivi;
- informazioni più strettamente connesse allo svolgimento dell'attività lavorativa, quali la tipologia del contratto (a tempo determinato o indeterminato, a tempo pieno o parziale, etc.); la qualifica e il livello professionale, la retribuzione individuale corrisposta anche in virtù di provvedimenti "ad personam"; l'ammontare di premi; il tempo di lavoro anche straordinario; ferie e permessi individuali (fruiti o residui); l'assenza dal servizio nei casi previsti dalla legge o dai contratti anche collettivi di lavoro; trasferimenti ad altra sede di lavoro; procedimenti e provvedimenti disciplinari.

I medesimi dati sono:

- contenuti in atti e documenti prodotti dai lavoratori in sede di assunzione (rispetto ai quali, con riferimento alle informazioni raccolte mediante annunci contenenti offerte di lavoro, questa Autorità si è già pronunciata [2] o nel corso del rapporto di lavoro;
- contenuti in documenti e/o file elaborati dal (o per conto del) datore di lavoro in pendenza del rapporto di lavoro per finalità di esecuzione del contratto e successivamente raccolti e conservati in fascicoli personali, archivi cartacei o elettronici aziendali [3];
- resi disponibili in albi e bacheche o, ancora, nelle intranet aziendali.

2. Il rispetto dei principi di protezione dei dati personali

2.1. Liceità, pertinenza, trasparenza. Le predette informazioni di carattere personale possono essere trattate dal datore di lavoro nella misura in cui siano necessarie per dare corretta esecuzione al rapporto di lavoro; talvolta, sono anche indispensabili per attuare previsioni contenute in leggi, regolamenti, contratti e accordi collettivi.
In ogni caso, deve trattarsi di informazioni pertinenti e non eccedenti e devono essere osservate tutte le disposizioni della vigente disciplina in materia di protezione dei dati personali che trae origine anche da direttive comunitarie.
In particolare, il Codice in materia di protezione dei dati personali (Codice), in attuazione delle direttive 95/46/Ce e 2002/58/Ce, prescrive che il trattamento di dati personali avvenga:

- nel rispetto di principi di necessità e liceità e che riguardano la qualità dei dati (artt. 3 e 11);
- informando preventivamente e adeguatamente gli interessati (art. 13);
- chiedendo preventivamente il consenso solo quando, anche a seconda della natura dei dati, non sia corretto avvalersi di uno degli altri presupposti equipollenti al consenso (artt. 23, 24, 26 e 43 del Codice);
- rispettando, se si trattano dati sensibili o giudiziari, le prescrizioni impartite dal Garante nelle autorizzazioni anche di carattere generale rilasciate (artt. 26 e 27 del Codice; cfr., in particolare, l'autorizzazione generale n. 1/2005);
- adottando le misure di sicurezza idonee a preservare i dati da alcuni eventi tra i quali accessi ed utilizzazioni indebite, rispetto ai quali può essere chiamato a rispondere anche civilmente e penalmente (artt. 15, 31 e ss., 167 e 169 del Codice).

2.2. Finalità. Il trattamento di dati personali riferibili a singoli lavoratori, anche sensibili, è lecito, se finalizzato ad assolvere obblighi derivanti dal contratto individuale (ad esempio, per verificare

l'esatto adempimento della prestazione o commisurare l'importo della retribuzione, anche per lavoro straordinario, o dei premi da corrispondere, per quantificare le ferie e i permessi, per appurare la sussistenza di una causa legittima di assenza).
Alcuni scopi sono altresì previsti dalla contrattazione collettiva per la determinazione di circostanze relative al rapporto di lavoro individuale (ad esempio, per la fruizione di permessi o aspettative sindacali e periodi di comporto o rispetto alle percentuali di lavoratori da assumere con particolari tipologie di contratto) o, ancora, dalla legge (quali, ad esempio, le comunicazioni ad enti previdenziali e assistenziali).
Se queste finalità sono in termini generali lecite, occorre però rispettare il principio della compatibilità tra gli scopi perseguiti (art. 11, comma 1, lett. b), del Codice): lo scopo perseguito in concreto dal datore di lavoro sulla base del trattamento di dati personali non deve essere infatti incompatibile con le finalità per le quali i medesimi sono stati raccolti.

3. Titolare e responsabile del trattamento

3.1. Titolare e responsabile. Ai fini della protezione dei dati personali assume un ruolo rilevante identificare le figure soggettive che a diverso titolo possono trattare i dati, definendo chiaramente le rispettive attribuzioni, in particolare, quelle del titolare e del responsabile del trattamento (artt. 4, comma 1, lett. f) e g), 28 e 29 del Codice).
In linea di principio, per individuare il titolare del trattamento rileva l'effettivo centro di imputazione del rapporto di lavoro, al di là dello schema societario formalmente adottato [4].
Peraltro, specie nelle realtà imprenditoriali più articolate, questa identificazione può risultare non sempre agevole e tale circostanza costituisce in qualche caso un ostacolo anche per l'esercizio dei diritti di cui all'art. 7 [5].

3.2. Gruppi di imprese. Le società che appartengono a gruppi di imprese individuati in conformità alla legge (art. 2359 cod. civ.; d.lg. 2 aprile 2002, n. 74) hanno di regola una distinta ed autonoma titolarità del trattamento in relazione ai dati personali dei propri dipendenti e collaboratori (artt. 4, comma 1, lett. f) e 28 del Codice).
Tuttavia, nell'ambito dei gruppi, le società controllate e collegate possono delegare la società capogruppo a svolgere adempimenti in materia di lavoro, previdenza ed assistenza sociale per i lavoratori indicati dalla legge [6]: tale attività implica la designazione della società capogruppo quale responsabile del trattamento ai sensi dell'art. 29 del Codice [7].
Analoga soluzione (art. 31, comma 2, d.lg. n. 276/2003) deve essere adottata per i trattamenti di dati personali, aventi identica natura, effettuati nell'ambito dei consorzi di società cooperative (nei quali a tal fine può essere altresì designata una delle società consorziate).

3.3. Medico competente. Considerazioni ulteriori devono essere svolte in relazione a taluni specifici trattamenti che possono o devono essere effettuati all'interno dell'impresa in conformità alla disciplina in materia di sicurezza e igiene del lavoro [8].
Tale disciplina, che attua anche alcune direttive comunitarie e si colloca nell'ambito del più generale quadro di misure necessarie a tutelare l'integrità psico-fisica dei lavoratori (art. 2087 cod. civ.), pone direttamente in capo al medico competente in materia di igiene e sicurezza dei luoghi di lavoro la sorveglianza sanitaria obbligatoria (e, ai sensi degli artt. 16 e 17 del d.lg. n. 626/1994, il correlativo trattamento dei dati contenuti in cartelle cliniche).
In quest'ambito, il medico competente effettua accertamenti preventivi e periodici sui lavoratori (art. 33 d.P.R. n. 303/1956; art. 16 d.lg. n. 626/1994) e istituisce (curandone l'aggiornamento) una cartella sanitaria e di rischio (in conformità alle prescrizioni contenute negli artt. 17, 59-*quinquiesdecies*, comma 2, lett. b), 59-sexiesdecies e 70 d.lg. n. 626/1994).
Detta cartella è custodita presso l'azienda o l'unità produttiva, "*con salvaguardia del segreto professionale, e* [consegnata in] *copia al lavoratore stesso al momento della risoluzione del rapporto di lavoro, ovvero quando lo stesso ne fa richiesta*" (art. 4, comma 8, d.lg. n. 626/1994); in

caso di cessazione del rapporto di lavoro le cartelle sono trasmesse all'Istituto superiore prevenzione e sicurezza sul lavoro-Ispesl (art. 72-*undecies*, comma 3, d.lg. n. 626/1994), in originale e in busta chiusa [9].
In relazione a tali disposizioni, il medico competente è deputato a trattare i dati sanitari dei lavoratori, procedendo alle dovute annotazioni nelle cartelle sanitarie e di rischio, e curando le opportune misure di sicurezza per salvaguardare la segretezza delle informazioni trattate in rapporto alle finalità e modalità del trattamento stabilite. Ciò, quale che sia il titolare del trattamento effettuato dal medico [10].
Alle predette cartelle il datore di lavoro non può accedere, dovendo soltanto concorrere ad assicurarne un'efficace custodia nei locali aziendali (anche in vista di possibili accertamenti ispettivi da parte dei soggetti istituzionalmente competenti), ma, come detto, "*con salvaguardia del segreto professionale*" [11].
Il datore di lavoro, sebbene sia tenuto, su parere del medico competente (o qualora il medico lo informi di anomalie imputabili all'esposizione a rischio), ad adottare le misure preventive e protettive per i lavoratori interessati, non può conoscere le eventuali patologie accertate, ma solo la valutazione finale circa l'idoneità del dipendente (dal punto di vista sanitario) allo svolgimento di date mansioni.
In tal senso, peraltro, depongono anche le previsioni legislative che dispongono la comunicazione all'Ispesl della cartella sanitaria e di rischio in caso di cessione (art. 59-*sexiesdecies*, comma 4, d.lg. n. 626/1994) o cessazione del rapporto di lavoro (art. 72-*undecies* d.lg. n. 626/1994), precludendosi anche in tali occasioni ogni loro conoscibilità da parte del datore di lavoro.

4. Dati biometrici e accesso ad "aree riservate"

4.1. Nozione. In più circostanze, anche ricorrendo al procedimento previsto dall'art. 17 del Codice, è stato prospettato al Garante l'utilizzo di dati biometrici sul luogo di lavoro [12], con particolare riferimento all'impiego di tali informazioni per accedere ad aree specifiche dell'impresa.
Si tratta di dati ricavati dalle caratteristiche fisiche o comportamentali della persona a seguito di un apposito procedimento (in parte automatizzato) e poi risultanti in un modello di riferimento. Quest'ultimo consiste in un insieme di valori numerici ricavati, attraverso funzioni matematiche, dalle caratteristiche individuali sopra indicate, preordinati all'identificazione personale attraverso opportune operazioni di confronto tra il codice numerico ricavato ad ogni accesso e quello originariamente raccolto.
L'uso generalizzato e incontrollato di dati biometrici, specie se ricavati dalle impronte digitali, non è lecito. Tali dati, per la loro peculiare natura, richiedono l'adozione di elevate cautele per prevenire possibili pregiudizi a danno degli interessati, con particolare riguardo a condotte illecite che determinino l'abusiva "ricostruzione" dell'impronta, partendo dal modello di riferimento, e la sua ulteriore "utilizzazione" a loro insaputa.
L'utilizzo di dati biometrici può essere giustificato solo in casi particolari, tenuto conto delle finalità e del contesto in cui essi sono trattati e, in relazione ai luoghi di lavoro, per presidiare accessi ad "aree sensibili", considerata la natura delle attività ivi svolte: si pensi, ad esempio, a processi produttivi pericolosi [13] o sottoposti a segreti di varia natura [14] o al fatto che particolari locali siano destinati alla custodia di beni, documenti segreti o riservati o oggetti di valore [15].

4.2. Sistemi di rilevazione biometrica . Inoltre, nei casi in cui l'uso dei dati biometrici è consentito, la centralizzazione in una banca dati delle informazioni personali (nella forma del predetto modello) trattate nell'ambito del descritto procedimento di riconoscimento biometrico risulta di regola sproporzionata e non necessaria. I sistemi informativi devono essere infatti configurati in modo da ridurre al minimo l'utilizzazione di dati personali e da escluderne il trattamento, quando le finalità perseguite possono essere realizzate con modalità tali da permettere di identificare l'interessato solo in caso di necessità (artt. 3 e 11 del Codice).

In luogo, quindi, di modalità centralizzate di trattamento dei dati biometrici, deve ritenersi adeguato e sufficiente avvalersi di sistemi efficaci di verifica e di identificazione biometrica basati sulla lettura delle impronte digitali memorizzate, tramite il predetto modello cifrato, su un supporto posto nell'esclusiva disponibilità dell'interessato (una *smart card* o un dispositivo analogo) e privo di indicazioni nominative riferibili a quest'ultimo (essendo sufficiente attribuire a ciascun dipendente un codice individuale).
Tale modalità di riconoscimento, infatti, è idonea ad assicurare che possano accedere all'area riservata solo coloro che, autorizzati preventivamente, decidano su base volontaria di avvalersi della predetta carta o del dispositivo analogo. Il confronto delle impronte digitali con il modello memorizzato sulla carta o sul dispositivo può essere realizzato ricorrendo a comuni procedure di confronto sulla carta o dispositivo stesso, evitando così la costituzione di un archivio di delicati dati biometrici. Del resto, in caso di smarrimento della carta o dispositivo, sono allo stato circoscritte le possibilità di abuso rispetto ai dati biometrici ivi memorizzati.

4.3. Misure di sicurezza e tempi di conservazione. I dati personali necessari per realizzare il modello possono essere trattati esclusivamente durante la fase di registrazione; per il loro utilizzo, il titolare del trattamento deve raccogliere il preventivo consenso informato degli interessati.
In aggiunta alle misure di sicurezza minime prescritte dal Codice, devono essere adottati ulteriori accorgimenti a protezione dei dati, impartendo agli incaricati apposite istruzioni scritte alle quali attenersi, con particolare riguardo al caso di perdita o sottrazione delle carte o dispositivi loro affidati.
I dati memorizzati devono essere accessibili al personale preposto al rispetto delle misure di sicurezza all'interno dell'impresa, per l'esclusiva finalità della verifica della loro osservanza (rispettando peraltro la disciplina sul controllo a distanza dei lavoratori: art. 4, comma 2, l. 20 maggio 1970, n. 300, richiamato dall'art. 114 del Codice).
I dati raccolti non possono essere di regola conservati per un arco di tempo superiore a sette giorni e vanno assicurati, anche quando tale arco temporale possa essere lecitamente protratto, idonei meccanismi di cancellazione automatica dei dati.

4.4. Verifica preliminare. Resta salva, per fattispecie particolari o in ragione di situazioni eccezionali non considerate in questa sede, la presentazione da parte di titolari del trattamento che intendano discostarsi dalle presenti prescrizioni, di apposito interpello al Garante, ai sensi dell'art. 17 del Codice.

5. Comunicazione e diffusione di dati personali

5.1. Comunicazione. La conoscenza dei dati personali relativi ad un lavoratore da parte di terzi è ammessa se l'interessato vi acconsente.
Se il datore di lavoro non può avvalersi correttamente di uno degli altri presupposti del trattamento equipollenti al consenso (art. 24 del Codice), non può prescindersi dal consenso stesso per comunicare dati personali (ad esempio, inerenti alla circostanza di un'avvenuta assunzione, allo *status* o alla qualifica ricoperta, all'irrogazione di sanzioni disciplinari o a trasferimenti del lavoratore) a terzi quali:

- associazioni (anche di categoria) di datori di lavoro, o di ex dipendenti (anche della medesima istituzione);
- conoscenti, familiari e parenti.

Fermo restando il rispetto dei principi generali sopra richiamati in materia di trattamento di dati personali (cfr. punto 2), rimane impregiudicata la facoltà del datore di lavoro di disciplinare le modalità del proprio trattamento designando i soggetti, interni o esterni, incaricati o responsabili del trattamento, che possono acquisire conoscenza dei dati inerenti alla gestione del rapporto di lavoro, in relazione alle funzioni svolte e a idonee istruzioni scritte alle quali attenersi (artt. 4, comma 1,

lett. g) e h), 29 e 30). Ciò, ove necessario, anche mediante consegna di copia di documenti all'uopo predisposti.
È altresì impregiudicata la facoltà del datore di lavoro di comunicare a terzi in forma realmente anonima dati ricavati dalle informazioni relative a singoli o gruppi di lavoratori: si pensi al numero complessivo di ore di lavoro straordinario prestate o di ore non lavorate a livello aziendale o all'interno di singole unità produttive, agli importi di premi aziendali di risultato individuati per fasce, o qualifiche/livelli professionali, anche nell'ambito di singole funzioni o unità organizzative).

5.2. Intranet aziendale. Allo stesso modo, il consenso del lavoratore è necessario per pubblicare informazioni personali allo stesso riferite (quali fotografia, informazioni anagrafiche o *curricula*) nella *intranet* aziendale (e a maggior ragione in *Internet*), non risultando tale ampia circolazione di dati personali di regola "*necessaria per eseguire obblighi derivanti dal contratto di lavoro* " (art. 24, comma 1, lett. b), del Codice). Tali obblighi possono trovare esecuzione indipendentemente da tale particolare forma di divulgazione che comunque, potendo a volte risultare pertinente (specie in realtà produttive di grandi dimensioni o ramificate sul territorio), richiede il preventivo consenso del singolo dipendente, salva specifica disposizione di legge.

5.3. Diffusione. In assenza di specifiche disposizioni normative che impongano al datore di lavoro la diffusione di dati personali riferiti ai lavoratori (art. 24, comma 1, lett. a) o la autorizzino, o comunque di altro presupposto ai sensi dell'art. 24 del Codice, la diffusione stessa può avvenire solo se necessaria per dare esecuzione a obblighi derivanti dal contratto di lavoro (art. 24, comma 1, lett. b) del Codice). È il caso, ad esempio, dell'affissione nella bacheca aziendale di ordini di servizio, di turni lavorativi o feriali, oltre che di disposizioni riguardanti l'organizzazione del lavoro e l'individuazione delle mansioni cui sono deputati i singoli dipendenti [16].
Salvo che ricorra una di queste ipotesi, non è invece di regola lecito dare diffusione a informazioni personali riferite a singoli lavoratori, anche attraverso la loro pubblicazione in bacheche aziendali o in comunicazioni interne destinate alla collettività dei lavoratori, specie se non correlate all'esecuzione di obblighi lavorativi. In tali casi la diffusione si pone anche in violazione dei principi di finalità e pertinenza (art. 11 del Codice), come nelle ipotesi di:

- affissione relativa ad emolumenti percepiti o che fanno riferimento a particolari condizioni personali [17];
- sanzioni disciplinari irrogate o informazioni relative a controversie giudiziarie;
- assenze dal lavoro per malattia;
- iscrizione e/o adesione dei singoli lavoratori ad associazioni.

5.4. Cartellini identificativi. Analogamente, si possono determinare altre forme di diffusione di dati personali quando dette informazioni debbano essere riportate ed esibite su cartellini identificativi appuntati ad esempio sull'abito o sulla divisa del lavoratore (di solito, con lo scopo di migliorare il rapporto fra operatori ed utenti o clienti).
Al riguardo, questa Autorità ha già rilevato [18], in relazione allo svolgimento del rapporto di lavoro alle dipendenze di soggetti privati, che l'obbligo di portare in modo visibile un cartellino identificativo può trovare fondamento in alcune prescrizioni contenute in accordi sindacali aziendali, il cui rispetto può essere ricondotto alle prescrizioni del contratto di lavoro. Tuttavia, in relazione al rapporto con il pubblico, si è ravvisata la sproporzione dell'indicazione sul cartellino di dati personali identificativi (generalità o dati anagrafici), ben potendo spesso risultare sufficienti altre informazioni (quali codici identificativi, il solo nome o il ruolo professionale svolto), per sé sole in grado di essere d'ausilio all'utenza.

5.5. Modalità di comunicazione. Salvi i casi in cui forme e modalità di divulgazione di dati personali discendano da specifiche previsioni (cfr. art. 174, comma 12, del Codice) [19], il datore di lavoro deve utilizzare forme di comunicazione individualizzata con il lavoratore, adottando le

misure più opportune per prevenire un'indebita comunicazione di dati personali, in particolare se sensibili, a soggetti diversi dal destinatario, ancorché incaricati di talune operazioni di trattamento (ad esempio, inoltrando le comunicazioni in plico chiuso o spillato; invitando l'interessato a ritirare personalmente la documentazione presso l'ufficio competente; ricorrendo a comunicazioni telematiche individuali).
Analoghe cautele, tenendo conto delle circostanze di fatto, devono essere adottate in relazione ad altre forme di comunicazione indirizzate al lavoratore dalle quali possano desumersi vicende personali [20].

6. Dati idonei a rivelare lo stato di salute di lavoratori

6.1. Dati sanitari. Devono essere osservate cautele particolari anche nel trattamento dei dati sensibili del lavoratore (art. 4, comma 1, lett. d), del Codice) e, segnatamente, di quelli dati idonei a rivelarne lo stato di salute. Tra questi ultimi, può rientrare l'informazione relativa all'assenza dal servizio per malattia, indipendentemente dalla circostanza della contestuale enunciazione della diagnosi [21].
Per tali informazioni, l'ordinamento appresta anche fuori della disciplina di protezione dei dati personali particolari accorgimenti per contenere, nei limiti dell'indispensabile, i dati dei quali il datore di lavoro può venire a conoscenza per dare esecuzione al contratto (cfr. già l'art. 8 della legge n. 300/1970).
In questo contesto, la disciplina generale contenuta nel Codice deve essere coordinata ed integrata, come si è visto (cfr. punto 3.3.), con altre regole settoriali [22] o speciali [23].
Resta comunque vietata la diffusione di dati sanitari (art. 26, comma 5, del Codice).

6.2. Assenze per ragioni di salute. Con specifico riguardo al trattamento di dati idonei a rivelare lo stato di salute dei lavoratori, la normativa di settore e le disposizioni contenute nei contratti collettivi giustificano il trattamento dei dati relativi ai casi di infermità (e talora a quelli inerenti all'esecuzione di visite specialistiche o di accertamenti clinici) che determini un'incapacità lavorativa (temporanea o definitiva, con la conseguente sospensione o risoluzione del contratto). Non diversamente, il datore di lavoro può trattare dati relativi a invalidità o all'appartenenza a categorie protette, nei modi e per le finalità prescritte dalla vigente normativa in materia.
A tale riguardo, infatti, sussiste un quadro normativo articolato che prevede anche obblighi di comunicazione in capo al lavoratore e di successiva certificazione nei confronti del datore di lavoro e dell'ente previdenziale della condizione di malattia: obblighi funzionali non solo a giustificare i trattamenti normativi ed economici spettanti al lavoratore, ma anche a consentire al datore di lavoro, nelle forme di legge [24], di verificare le reali condizioni di salute del lavoratore.
Per attuare tali obblighi viene utilizzata un'apposita modulistica, consistente in un attestato di malattia da consegnare al datore di lavoro –con la sola indicazione dell'inizio e della durata presunta dell'infermità: c.d. "prognosi"– e in un certificato di diagnosi da consegnare, a cura del lavoratore stesso, all'Istituto nazionale della previdenza sociale (Inps) o alla struttura pubblica indicata dallo stesso Istituto d'intesa con la regione, se il lavoratore ha diritto a ricevere l'indennità di malattia a carico dell'ente previdenziale [25].
Tuttavia, qualora dovessero essere presentati dai lavoratori certificati medici redatti su modulistica diversa da quella sopra descritta, nella quale i dati di prognosi e di diagnosi non siano separati, i datori di lavoro restano obbligati, ove possibile, ad adottare idonee misure e accorgimenti volti a prevenirne la ricezione o, in ogni caso, ad oscurali [26].

6.3. Denuncia all'Inail. Diversamente, per dare esecuzione ad obblighi di comunicazione relativi a dati sanitari, in taluni casi il datore di lavoro può anche venire a conoscenza delle condizioni di salute del lavoratore.
Tra le fattispecie più ricorrenti deve essere annoverata la denuncia all'Istituto assicuratore (Inail) avente ad oggetto infortuni e malattie professionali occorsi ai lavoratori; essa, infatti, per espressa

previsione normativa, deve essere corredata da specifica certificazione medica (artt. 13 e 53 d.P.R. n. 1124/1965).
In tali casi, pur essendo legittima la conoscenza della diagnosi da parte del datore di lavoro, resta fermo a suo carico l'obbligo di limitarsi a comunicare all'ente assistenziale esclusivamente le informazioni sanitarie relative o collegate alla patologia denunciata e non anche dati sulla salute relativi ad altre assenze che si siano verificate nel corso del rapporto di lavoro, la cui eventuale comunicazione sarebbe eccedente e non pertinente –con la conseguente loro inutilizzabilità–, trattandosi di dati non rilevanti nel caso oggetto di denuncia (art. 11, commi 1 e 2 del Codice) [27].

6.4. Altre informazioni relative alla salute. A tali fattispecie devono essere aggiunti altri casi nei quali può, parimenti, effettuarsi un trattamento di dati relativi alla salute del lavoratore (e finanche di suoi congiunti), anche al fine di permettergli di godere dei benefici di legge (quali, ad esempio, permessi o periodi prolungati di aspettativa con conservazione del posto di lavoro): si pensi, ad esempio, a informazioni relative a condizioni di *handicap* [28].
Allo stesso modo, il datore di lavoro può venire a conoscenza dello stato di tossicodipendenza del dipendente, ove questi richieda di accedere a programmi riabilitativi o terapeutici con conservazione del posto di lavoro (senza retribuzione), atteso l'onere di presentare (nei termini prescritti dai contratti collettivi) specifica documentazione medica al datore di lavoro (ai sensi dell'art. 124, commi 1 e 2, d.P.R. n. 309/1990).

6.5. Comunicazioni all'Inps. È altresì legittima la comunicazione di dati idonei a rivelare lo stato di salute dei lavoratori che il datore di lavoro faccia ai soggetti pubblici (enti previdenziali e assistenziali) tenuti a erogare le prescritte indennità in adempimento a specifici obblighi derivanti dalla legge, da altre norme o regolamenti o da previsioni contrattuali, nei limiti delle sole informazioni indispensabili.
In particolare, il datore di lavoro può comunicare all'Istituto nazionale della previdenza sociale (Inps) i dati del dipendente assente, anche per un solo giorno, al fine di farne controllare lo stato di malattia (art. 5, commi 1 e 2, l. 20 maggio 1970, n. 300) [29]; a tal fine deve tenere a disposizione e produrre, a richiesta, all'Inps, la documentazione in suo possesso. Le eventuali visite di controllo sullo stato di infermità del lavoratore, ai sensi dell'art. 5 della legge 20 maggio 1970, n. 300, o su richiesta dell'Inps o della struttura sanitaria pubblica da esso indicata, sono effettuate dai medici dei servizi sanitari indicati dalle regioni (art. 2, l. n. 33/1980 cit.).

7. Informativa

Il datore di lavoro è tenuto a rendere al lavoratore, prima di procedere al trattamento dei dati personali che lo riguardano (anche in relazione alle ipotesi nelle quali la legge non richieda il suo consenso), un'informativa individualizzata completa degli elementi indicati dall'art. 13 del Codice [30].
Con particolare riferimento a realtà produttive nelle quali, per ragioni organizzative (ad esempio, per l'articolata dislocazione sul territorio o per il ricorso consistente a forme di out-sourcing) o dimensionali, può risultare difficoltoso per il singolo lavoratore esercitare i propri diritti ai sensi dell'art. 7 del Codice, è opportuna la designazione di un responsabile del trattamento appositamente deputato alla trattazione di tali profili (o di responsabili esterni alla società, che effettuino, ad esempio, l'attività di gestione degli archivi amministrativi dei dipendenti), indicandolo chiaramente nell'informativa fornita.

8. Misure di sicurezza

8.1. Dati sanitari. Il datore di lavoro titolare del trattamento è tenuto ad adottare ogni misura di sicurezza, anche minima, prescritta dal Codice a protezione dei dati personali dei dipendenti

comunque trattati nell'ambito del rapporto di lavoro, ponendo particolare attenzione all'eventuale natura sensibile dei medesimi (art. 31 ss. e Allegato B) al Codice).
Dette informazioni devono essere conservate separatamente da ogni altro dato personale dell'interessato; ciò, deve trovare attuazione anche con riferimento ai fascicoli personali cartacei dei dipendenti (ad esempio, utilizzando sezioni appositamente dedicate alla custodia dei dati sensibili, inclusi quelli idonei a rivelare lo stato di salute del lavoratore, da conservare separatamente o in modo da non consentirne una indistinta consultazione nel corso delle ordinarie attività amministrative [31]).
Del pari, nei casi in cui i lavoratori producano spontaneamente certificati medici su modulistica diversa da quella descritta al punto 6.2., il datore di lavoro non può, comunque, utilizzare ulteriormente tali informazioni (art. 11, comma 2, del Codice) e deve adottare gli opportuni accorgimenti per non rendere visibili le diagnosi contenute nei certificati (ad esempio, prescrivendone la circolazione in busta chiusa previo oscuramento di tali informazioni); ciò, al fine di impedire ogni accesso abusivo a tali dati da parte di soggetti non previamente designati come incaricati o responsabili (art. 31 e ss. del Codice).

8.2. Incaricati. Resta fermo l'obbligo del datore di lavoro di preporre alla custodia dei dati personali dei lavoratori apposito personale, specificamente incaricato del trattamento, che "*deve avere cognizioni in materia di protezione dei dati personali e ricevere una formazione adeguata. In assenza di un'adeguata formazione degli addetti al trattamento dei dati personali il rispetto della riservatezza dei lavoratori sul luogo di lavoro non potrà mai essere garantito*" [32].

8.3. Misure fisiche ed organizzative. Il datore di lavoro deve adottare, tra l'altro (cfr. artt. 31 ss. del Codice), misure organizzative e fisiche idonee a garantire che:

- i luoghi ove si svolge il trattamento di dati personali dei lavoratori siano opportunamente protetti da indebite intrusioni;
- le comunicazioni personali riferibili esclusivamente a singoli lavoratori avvengano con modalità tali da escluderne l'indebita presa di conoscenza da parte di terzi o di soggetti non designati quali incaricati;
- siano impartite chiare istruzioni agli incaricati in ordine alla scrupolosa osservanza del segreto d'ufficio, anche con riguardo a dipendenti del medesimo datore di lavoro che non abbiano titolo per venire a conoscenza di particolari informazioni personali;
- sia prevenuta l'acquisizione e riproduzione di dati personali trattati elettronicamente, in assenza di adeguati sistemi di autenticazione o autorizzazione e/o di documenti contenenti informazioni personali da parte di soggetti non autorizzati [33];
- sia prevenuta l'involontaria acquisizione di informazioni personali da parte di terzi o di altri dipendenti: opportuni accorgimenti, ad esempio, devono essere presi in presenza di una particolare conformazione o dislocazione degli uffici, in assenza di misure idonee volte a prevenire la diffusione delle informazioni (si pensi al mancato rispetto di distanze di sicurezza o alla trattazione di informazioni riservate in spazi aperti, anziché all'interno di locali chiusi).

9. Esercizio dei diritti previsti dall'art. 7 del Codice e riscontro del datore di lavoro

9.1. Diritto di accesso. I lavoratori interessati possono esercitare nei confronti del datore di lavoro i diritti previsti dall'art. 7 del Codice (nei modi di cui agli artt. 8 e ss.), tra cui il diritto di accedere ai dati che li riguardano (anziché, in quanto tale, all'intera documentazione che li contiene [34]), di ottenerne l'aggiornamento, la rettificazione, l'integrazione, la cancellazione, la trasformazione in forma anonima o il blocco se trattati in violazione di legge, di opporsi al trattamento per motivi legittimi.
La richiesta di accesso che non faccia riferimento ad un particolare trattamento o a specifici dati o categorie di dati, deve ritenersi riferita a tutti i dati personali che riguardano il lavoratore comunque

trattati dall'amministrazione (art. 10) e può riguardare anche informazioni di tipo valutativo [35], alle condizioni e nei limiti di cui all'art. 8, comma 5.
Tra essi non rientrano notizie di carattere contrattuale o professionale che non hanno natura di dati personali in qualche modo riferibili a persone identificate o identificabili [36].

9.2. Riscontro del datore di lavoro. Il datore di lavoro destinatario della richiesta è tenuto a fornire un riscontro completo alla richiesta del lavoratore interessato, senza limitarsi alla sola elencazione delle tipologie di dati detenuti, ma comunicando in modo chiaro e intelligibile tutte le informazioni in suo possesso [37].

9.3. Tempestività del riscontro. Il riscontro deve essere fornito nel termine di 15 giorni dal ricevimento dell'istanza dell'interessato (ritualmente presentata [38]); il termine più lungo, pari a 30 giorni, può essere osservato, dandone comunicazione all'interessato, solo se le operazioni necessarie per un integrale riscontro sono di particolare complessità o se ricorre altro giustificato motivo (art. 146 del Codice).
Pertanto il datore di lavoro, specie nelle realtà produttive di grande dimensione [39], deve pertanto predisporre procedure organizzative adeguate per dare piena attuazione alle disposizioni del Codice in materia di accesso ai dati e all'esercizio degli altri diritti, anche attraverso l'impiego di appositi programmi finalizzati ad una accurata selezione dei dati relativi a singoli lavoratori, nonché alla semplificazione delle modalità e alla compressione dei tempi per il riscontro.

9.4. Modalità del riscontro. Il riscontro può essere fornito anche oralmente; tuttavia, in presenza di una specifica istanza, il datore di lavoro è tenuto a trasporre i dati su supporto cartaceo o informatico o a trasmetterli all'interessato per via telematica (art. 10).
Muovendo dalla previsione dell'art. 10, comma 1, del Codice, secondo cui il titolare deve predisporre accorgimenti idonei "a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente", può risultare legittima la richiesta dell'interessato di ricevere la comunicazione dei dati in questione presso la propria sede lavorativa o la propria abitazione [40].

9.5. Dati personali e documentazione. Come più volte dichiarato dal Garante [41], l'esercizio del diritto di accesso consente di ottenere, ai sensi dell'art. 10 del Codice, solo la comunicazione dei dati personali relativi al richiedente detenuti dal titolare del trattamento e da estrarre da atti e documenti; non permette invece di richiedere a quest'ultimo il diretto e illimitato accesso a documenti e ad intere tipologie di atti, o la creazione di documenti allo stato inesistenti negli archivi, o la loro innovativa aggregazione secondo specifiche modalità prospettate dall'interessato o, ancora, di ottenere, sempre e necessariamente, copia dei documenti detenuti, ovvero di pretendere particolari modalità di riscontro (salvo quanto previsto per la trasposizione dei dati su supporto cartaceo: cfr. art. 10, comma 2, del Codice).
Specie nei casi in cui è elevata la mole di informazioni personali detenute dal titolare del trattamento, il diritto di accesso ai dati può essere soddisfatto mettendo a disposizione dell'interessato il fascicolo personale [42], dal quale successivamente possono essere estratte le informazioni personali.
La scelta circa l'eventuale esibizione o consegna in copia di atti e documenti contenenti i dati personali richiesti può essere effettuata dal titolare del trattamento nel solo caso in cui l'estrapolazione dei dati personali da tali documenti risulti particolarmente difficoltosa per il titolare medesimo [43]; devono essere poi omessi eventuali dati personali riferiti a terzi (art. 10, comma 4, del Codice) [44]. L'adozione di tale modalità di riscontro non comporta l'obbligo in capo al titolare di fornire copia di tutti i documenti che contengano i medesimi dati personali dell'interessato, quando gli stessi dati siano conservati in più atti, lettere o note.
Nel fornire riscontro ad una richiesta di accesso formulata ai sensi degli artt. 7 e 8 del Codice, il titolare del trattamento deve, poi, comunicare i dati richiesti ed effettivamente detenuti, e non è

tenuto a ricercare o raccogliere altri dati che non siano nella propria disponibilità e non siano oggetto, in alcuna forma, di attuale trattamento da parte dello stesso (o perché originariamente trattati e non più disponibili, ovvero perché, come nel caso di dati contenuti nella corrispondenza intercorsa, in qualunque forma, tra dipendenti di un determinato datore di lavoro, non siano mai stati nell'effettiva e libera disponibilità di quest'ultimo (si pensi al caso di dati contenuti nella corrispondenza intercorsa tra dipendenti [45]) –al di là dei profili di tutela della segretezza della corrispondenza che pur vengono in rilievo–, non competerebbero le decisioni in ordine alle loro finalità e modalità di trattamento (cfr. art. 4, comma 1, lett. f), del Codice).

9.6. Aggiornamento. Infine, il lavoratore può ottenere l'aggiornamento dei dati personali a sé riferiti [46].
In ordine, poi, all'eventuale richiesta di rettifica dei dati personali indicati nel profilo professionale del lavoratore, la medesima può avvenire solo in presenza della prova dell'effettiva e legittima attribuibilità delle qualifiche rivendicate dall'interessato, ad esempio in base a "decisioni o documenti del datore di lavoro o di terzi, obblighi derivanti dal contratto di lavoro, provvedimenti di organi giurisdizionali relativi all'interessato o altri titoli o atti che permettano di ritenere provata, agli effetti e sul piano dell'applicazione della [disciplina di protezione dei dati personali], la richiesta dell'interessato" (che può comunque far valere in altra sede, sulla base di idoneo materiale probatorio, la propria pretesa al riconoscimento della qualifica o mansione rivendicata) [47].

NOTE:
1. Le indicazioni rese tengono altresì conto, per i profili esaminati, della Raccomandazione n. R (89) 2 del Consiglio d'Europa relativa alla protezione dei dati a carattere personale utilizzati ai fini dell'occupazione, del Parere 8/2001*sul trattamento dei dati personali nel contesto dell'occupazione*, reso il 13 settembre 2001 dal Gruppo dei Garanti europei, in http://ec.europa.eu e del Code of practice, "*Protection of workers' personal data* ", pubblicato dall'Organizzazione internazionale del lavoro (ILO).
2. Cfr. *Provv.* 10 gennaio 2002, in, doc. *web* n. 1064553
3. Cfr. *Provv.* 23 aprile 2002, doc. *web* n. 1065065
4. Cfr., in merito, i principi affermati in giurisprudenza: Cass. 24 marzo 2003, n. 4274; v. altresì Cass. 1° aprile 1999, n. 3136
5. In merito v. di seguito il punto 9
6. Cfr. art. 1 della legge 11 gennaio 1979, n. 12; cfr. art. 31, comma 1, d.lg. 10 settembre 2003, n. 276; l. 14 febbraio 2003, n. 30
7. Come già accade per i soggetti indicati al menzionato art. 1 della legge n. 12/1979
8. In particolare, d.lg. 19 settembre 1994, n. 626 e successive modificazioni e integrazioni
9. Cfr. circolare Ispesl 3 marzo 2003, n. 2260
10. In tal senso, v. l' autorizzazione generale n. 1/2005, in rapporto al diverso titolo in base al quale il medico opera quale libero professionista, o quale dipendente del datore di lavoro o di aziende sanitarie locali.
11. La cui violazione è peraltro penalmente sanzionata ai sensi dell'art. 92, lett. a), d.lg. n. 626/1994
12. Cfr. *Provv.* 21 luglio 2005, doc. *web* n. 1150679
13. Cfr. *Provv.* 15 giugno 2006, docc. *web* nn. 1306523, 1306530 e 1306551
14. Cfr. *Provv.* 23 novembre 2005, doc. *web* n. 1202254
15. Cfr. *Provv.* 15 giugno 2006, doc. *web* n. 1306098; v., inoltre, *Provv.* 26 luglio 2006, doc. *web* n. 1318582
16. Cfr. Cass., sez. lav., 24 novembre 1997, n. 11741; Cass., sez. lav., 11 febbraio 2000, n. 1557; Cass., sez. lav., 16 febbraio 2000, n. 1752
17. Cfr., in relazione alla diffusione di informazioni in grado di rivelare situazioni di *handicap*, *Provv.* 27 febbraio 2002, in *Boll.* n. 25/2002, p. 51, doc. *web* n. 1063639
18. Cfr. *Provv.* 11 dicembre 2000, doc. *web* n. 30991

19. Cfr. *Provv.* 12 maggio 2005, doc. *web* n. 1137798
20. Cfr., con riguardo alle dizioni riportate sui "cedolini" dello stipendio, o su documenti aventi la medesima funzione, *Provv.* 31 dicembre 1998, in *Boll.* n. 6, p. 100; v. anche *Provv.* 19 febbraio 2002, doc. *web* n. 1063659
21. Cfr. *Provv.* 7 luglio 2004, doc. *web* n. 1068839. V. pure il punto 50 della sentenza della Corte di giustizia delle Comunità europee, 6 novembre 2003, C-101/01, *Lindqvist*
22. Tra le quali, ad esempio, la richiamata regolamentazione contenuta nel d.lg. n. 626/1994 o nell'art. 5 della legge n. 300/1970 sugli accertamenti sanitari facoltativi
23. Si pensi, ad esempio, ai divieti contenuti negli artt. 5 e 6 della legge 5 giugno 1990, n. 135, in materia Aids; art. 124 d.P.R. 9 ottobre 1990, n. 309
24. Cfr. *Provv.* 15 aprile 2004, doc. *web* n. 1092564
25. Cfr. art. 2, d.l. 30 dicembre 1979, n. 663, conv. in l., con mod., con l'art. 1, l. 29 febbraio 1980, n. 33 e mod. dal comma 149 dell'art. 1, l. 30 dicembre 2004, n. 311
26. Cfr. di seguito al punto 8
27. In tal senso v. il *Provv.* 15 aprile 2004, doc. *web* n. 1092564
28. Cfr. art. 33, legge 5 febbraio 1992, n. 104; si vedano anche le pertinenti disposizioni contenute nel d.lg. 26 marzo 2001, n. 151
29. V. *Provv.* 28 settembre 2001, cit
30. V. anche il Parere 8/2001, cit., secondo il quale "*i lavoratori devono conoscere quali dati il datore di lavoro stia raccogliendo sul loro conto (direttamente o da altre fonti), quali siano gli scopi delle operazioni di trattamento previste o effettuate per tali dati sia per il presente che per il futuro* ".
31. Cfr. *Provv.* 30 ottobre 2001, doc. *web* n. 39085
32. Parere 8/2001, cit.)
33. Cfr. *Provv.* 27 luglio 2004, doc. *web* n. 1099386
34. Cfr. *Provv.* 16 giugno 2005, doc. *web* n. 1149957
35. V. già *Provv.* 7 marzo 2001, doc. *web* n. 40285; cfr. *Provv.* 15 novembre 2004, doc. *web* n. 1102939. Raccomandazione n. 1/2001 concernente i dati relativi alla valutazione del personale del Gruppo art. 29, Wp 42.
36. In tal senso, con riguardo ad esempio alle mansioni proprie di un determinato profilo professionale cfr. *Provv.* 29 ottobre 2003, doc. *web* n. 1053781
37. In tal senso cfr., in relazione ad informazioni personali conservate con tecniche di cifratura, *Provv.* 21 novembre 2001, doc. *web* n. 39773
38. Cfr. *Provv.* 17 febbraio 2005, doc. *web* n. 1148228, con il quale si è dichiarato inammissibile un ricorso presentato a seguito di istanza avanzata dalle "segreterie nazionali" di alcune organizzazioni sindacali priva di sottoscrizione.
39. Cfr. ad esempio *Provv.* 2 luglio 2003, doc. *web* n. 1079989; *Provv.* 24 giugno 2003, doc. *web* n. 1132725
40. Cfr. *Provv.* 17 marzo 2005, doc. *web* n. 1170467
41. Cfr. da ultimo *Provv.* 7 luglio 2005, doc. *web* n. 1149559; *Provv.* 16 giugno 2005, doc. *web* n. 1149999
42. *Provv.* 16 ottobre 2002, doc. *web* n. 1066447
43. Cfr. *Provv.* 25 novembre 2002, doc. *web* n. 1067321
44. Cfr. *Provv.* 20 aprile 2005, doc. *web* n. 1134190; già *Provv.* 27 dicembre 2001, in Boll., 2001, n. 23, p. 72
45. Cfr. *Provv.* 21 dicembre 2005, doc. *web* n. 1219039
46. Cfr., in relazione all'aggiornamento del dato relativo al titolo di studio, *Provv.* 6 settembre 2002, doc. *web* n. 1066183
47. Cfr., in relazione all'aggiornamento delle informazioni relative al titolo di studio, *Provv.* 9 gennaio 2003, doc. *web* n. 1067817

2.4. Lavoro: le linee guida del Garante per posta elettronica e internet

Gazzetta Ufficiale n. 58 del 10 marzo 2007

Del. n. 13 del 1° marzo 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Giuseppe Fortunato e del dott. Mauro Paissan, componenti, e del dott. Giovanni Buttarelli, segretario generale;
Visti i reclami, le segnalazioni e i quesiti pervenuti riguardo ai trattamenti di dati personali effettuati da datori di lavoro riguardo all'uso, da parte di lavoratori, di strumenti informatici e telematici;
Vista la documentazione in atti;
Visti gli artt. 24 e 154, comma 1, lett. b) e c) del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);
Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;
Relatore il dott. Mauro Paissan;

PREMESSO

1. Utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro

1.1. *Premessa*

Dall'esame di diversi reclami, segnalazioni e quesiti è emersa l'esigenza di prescrivere ai datori di lavoro alcune misure, necessarie o opportune, per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet.
Occorre muovere da alcune premesse:
a) compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;
b) spetta ad essi adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità (*artt. 15, 31 ss., 167 e 169 del Codice*);
c) emerge l'esigenza di tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;
d) l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di *log file* della navigazione *web* ottenuti, ad esempio, da un *proxy server* o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di *log file* di traffico *e-mail* e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;
e) le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili. (1)

1.2. *Tutela del lavoratore*

Le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi. La linea di confine tra questi ambiti, come

affermato dalla Corte europea dei diritti dell'uomo, può essere tracciata a volte solo con difficoltà. (2)

Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (*artt. 2 e 41, secondo comma, Cost.; art. 2087 cod. civ.; cfr. altresì l'art. 2, comma 5, Codice dell'amministrazione digitale (d.lg. 7 marzo 2005, n. 82), riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato*). (3)
Non a caso, nell'organizzare l'attività lavorativa e gli strumenti utilizzati, diversi datori di lavoro hanno prefigurato modalità d'uso che, tenendo conto del crescente lavoro in rete e di nuove tariffe di traffico forfettarie, assegnano aree di lavoro riservate per appunti strettamente personali, ovvero consentono usi moderati di strumenti per finalità private.

2. Codice in materia di protezione dei dati e discipline di settore

2.1. *Principi generali*

Nell'impartire le seguenti prescrizioni il Garante tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia (*artt. 1 e 2 del Codice*). Le prescrizioni potranno essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica.

2.2. *Discipline di settore*

Alcune disposizioni di settore, fatte salve dal Codice, prevedono specifici divieti o limiti, come quelli posti dallo Statuto dei lavoratori sul controllo a distanza (*artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 l. 20 maggio 1970, n. 300*).
La disciplina di protezione dei dati va coordinata con regole di settore riguardanti il rapporto di lavoro e il connesso utilizzo di tecnologie, nelle quali è fatta salva o richiamata espressamente (*art. 47, comma 3, lett. b) Codice dell'amministrazione digitale*). (4)

2.3. *Principi del Codice*

I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza di alcuni cogenti principi:
a) il principio di *necessità*, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (*art. 3 del Codice; par. 5.2*);
b) il principio di *correttezza*, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (*art. 11, comma 1, lett. a), del Codice*). Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati (*v. par. 3*);
c) i trattamenti devono essere effettuati per finalità *determinate*, *esplicite* e *legittime* (*art. 11, comma 1, lett. b), del Codice: par. 4 e 5*), osservando il principio di *pertinenza* e *non eccedenza* (*par. 6*). Il datore di lavoro deve trattare i dati *"nella misura meno invasiva possibile"*; le attività di monitoraggio devono essere svolte solo da soggetti preposti (*par. 8*) ed essere *"mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza"* (*Parere n. 8/2001, cit., punti 5 e 12*).

3. Controlli e correttezza nel trattamento

3.1. *Disciplina interna*

In base al richiamato principio di correttezza, l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore (*art. 4, secondo comma, Statuto dei lavoratori;allegato VII, par. 3 d.lg. n. 626/1994 e successive integrazioni e modificazioni in materia di "uso di attrezzature munite di videoterminali", il quale esclude la possibilità del controllo informatico "all'insaputa dei lavoratori"*). [(5)]
Grava quindi sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli. Ciò, tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali.
Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando il personale con modalità diverse anche a seconda delle dimensioni della struttura, tenendo conto, ad esempio, di piccole realtà dove vi è una continua condivisione interpersonale di risorse informative.

3.2. *Linee guida*

In questo quadro, può risultare opportuno adottare un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori, ecc.) e da sottoporre ad aggiornamento periodico.
A seconda dei casi andrebbe ad esempio specificato:

- se determinati comportamenti non sono tollerati rispetto alla "navigazione" in Internet (ad es., il *download* di *software* o di *file* musicali), oppure alla tenuta di file nella rete interna;
- in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di *webmail*, indicandone le modalità e l'arco temporale di utilizzo (ad es., fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
- quali informazioni sono memorizzate temporaneamente (ad es., le componenti di *file* di *log* eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;
- se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di *back up*, della gestione tecnica della rete o di *file* di *log*);
- se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime –specifiche e non generiche– per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet sono utilizzate indebitamente;
- le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;
- se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato;
- quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali;
- le prescrizioni interne sulla sicurezza dei dati e dei sistemi (*art. 34 del Codice, nonché Allegato B), in particolare regole 4, 9, 10*).

3.3. *Informativa (art. 13 del Codice)*
All'onere del datore di lavoro di prefigurare e pubblicizzare una *policy* interna rispetto al corretto uso dei mezzi e agli eventuali controlli, si affianca il dovere di informare comunque gli interessati ai sensi dell'art. 13 del Codice, anche unitamente agli elementi indicati ai punti 3.1. e 3.2..
Rispetto a eventuali controlli gli interessati hanno infatti il diritto di essere informati preventivamente, e in modo chiaro, sui trattamenti di dati che possono riguardarli.
Le finalità da indicare possono essere connesse a specifiche esigenze organizzative, produttive e di sicurezza del lavoro, quando comportano un trattamento lecito di dati (*art. 4, secondo comma, l. n. 300/1970*); possono anche riguardare l'esercizio di un diritto in sede giudiziaria.
Devono essere tra l'altro indicate le principali caratteristiche dei trattamenti, nonché il soggetto o l'unità organizzativa ai quali i lavoratori possono rivolgersi per esercitare i propri diritti.

4. Apparecchiature preordinate al controllo a distanza
Con riguardo al principio secondo cui occorre perseguire finalità determinate, esplicite e legittime (*art. 11, comma 1, lett. b), del Codice*), il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (*cfr. artt. 2086, 2087 e 2104 cod. civ.*).
Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare *"apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori"* (*art. 4, primo comma, l. n. 300/1970*), tra cui sono certamente comprese strumentazioni *hardware* e *software* mirate al controllo dell'utente di un sistema di comunicazione elettronica.
Il trattamento dei dati che ne consegue è illecito, a prescindere dall'illiceità dell'installazione stessa. Ciò, anche quando i singoli lavoratori ne siano consapevoli. (6)
In particolare non può ritenersi consentito il trattamento effettuato mediante sistemi *hardware* e *software* preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire –a volte anche minuziosamente– l'attività di lavoratori. É il caso, ad esempio:

- della lettura e della registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
- della riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
- della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- dell'analisi occulta di computer portatili affidati in uso.

Il controllo a distanza vietato dalla legge riguarda l'attività lavorativa in senso stretto e altre condotte personali poste in essere nel luogo di lavoro. (7) A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili (*art. 11, comma 2, del Codice*). (8)

5. Programmi che consentono controlli "indiretti"
5.1. Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (ad es., per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (*art. 4, comma 2*), di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. (9) Ciò, anche in presenza di attività di controllo discontinue. (10)
Il trattamento di dati che ne consegue può risultare lecito. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati (11), nonché in caso di

introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. (12)

5.2. *Principio di necessità*

In applicazione del menzionato principio di necessità il datore di lavoro è chiamato a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri (da preferire rispetto all'adozione di misure "repressive") e, comunque, a "minimizzare" l'uso di dati riferibili ai lavoratori *(artt. 3, 11, comma 1, lett. d) e 22, commi 3 e 5, del Codice; aut. gen. al trattamento dei dati sensibili n. 1/2005, punto 4)*.

Dal punto di vista organizzativo è quindi opportuno che:

- si valuti attentamente l'impatto sui diritti dei lavoratori (prima dell'installazione di apparecchiature suscettibili di consentire il controllo a distanza e dell'eventuale trattamento);
- si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e l'accesso a Internet; (13)
- si determini quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego abusivo.

Il datore di lavoro ha inoltre l'onere di adottare tutte le misure *tecnologiche* volte a minimizzare l'uso di dati identificativi (c.d. *privacy enhancing technologies–PETs*). Le misure possono essere differenziate a seconda della tecnologia impiegata (ad es., posta elettronica o navigazione in Internet).

a) Internet: la navigazione web

Il datore di lavoro, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'*upload* o il *download* di *file*, l'uso di servizi di rete con finalità ludiche o estranee all'attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. Tali controlli, leciti o meno a seconda dei casi, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale (*art. 8 l. n. 300/1970; artt. 26 e 113 del Codice; Provv. 2 febbraio 2006, cit.*).

In particolare, il datore di lavoro può adottare una o più delle seguenti misure opportune, tenendo conto delle peculiarità proprie di ciascuna organizzazione produttiva e dei diversi profili professionali:

- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni –reputate inconferenti con l'attività lavorativa– quali l'*upload* o l'accesso a determinati siti (inseriti in una sorta di *black list*) e/o il *download* di *file* o *software* aventi particolari caratteristiche (dimensionali o di tipologia di dato);
- trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai *file* di *log* riferiti al traffico *web*, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

b) Posta elettronica

Il contenuto dei messaggi di posta elettronica –come pure i dati esteriori delle comunicazioni e i *file* allegati– riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui *ratio* risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (*artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'amministrazione digitale*). (14)

Tuttavia, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando

quale espressione dell'organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa.
La mancata esplicitazione di una *policy* al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione.
Tali incertezze si riverberano sulla qualificazione, in termini di liceità, del comportamento del datore di lavoro che intenda apprendere il contenuto di messaggi inviati all'indirizzo di posta elettronica usato dal lavoratore (posta "in entrata") o di quelli inviati da quest'ultimo (posta "in uscita").
É quindi particolarmente opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Si tratta di soluzioni che possono risultare utili per contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza.
In questo quadro è opportuno che:

- il datore di lavoro renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it, ufficioreclami@società.com, urp@ente.it, etc.), eventualmente affiancandoli a quelli individuali (ad esempio, m.rossi@ente.it, rossi@società.com, mario.rossi@società.it);
- il datore di lavoro valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore; (15)
- il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. É parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica. (16) In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi *webmail*), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati;
- in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta *policy* datoriale.

6. Pertinenza e non eccedenza

6.1. *Graduazione dei controlli*

Nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.
L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali.
Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.
Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.
Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

6.2. *Conservazione*

I sistemi *software* devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei *log file*) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.
In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario –e predeterminato– a raggiungerla (*v. art. 11, comma 1, lett. e), del Codice*).
Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali (tenendo conto, con riguardo ai dati sensibili, delle prescrizioni contenute nelle autorizzazioni generali nn. 1/2005 e 5/2005 adottate dal Garante) deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

7. Presupposti di liceità del trattamento: bilanciamento di interessi

7.1. *Datori di lavoro privati*

I datori di lavoro privati e gli enti pubblici economici, se ricorrono i presupposti sopra indicati (*v., in particolare, art. 4, secondo comma, dello Statuto*), possono effettuare lecitamente il trattamento dei dati personali diversi da quelli sensibili.
Ciò, può avvenire:
a) se ricorrono gli estremi del legittimo esercizio di un diritto in sede giudiziaria (*art. 24, comma 1, lett. f) del Codice*);
b) in caso di valida manifestazione di un libero consenso;
c) anche in assenza del consenso, ma per effetto del presente provvedimento che individua un legittimo interesse al trattamento in applicazione della disciplina sul c.d. bilanciamento di interessi (*art. 24, comma 1, lett. g), del Codice*).
Per tale bilanciamento si è tenuto conto delle garanzie che lo Statuto prevede per il controllo "indiretto" a distanza presupponendo non il consenso degli interessati, ma un accordo con le rappresentanze sindacali (o, in difetto, l'autorizzazione di un organo periferico dell'amministrazione del lavoro).
L'eventuale trattamento di dati sensibili è consentito con il consenso degli interessati o, senza il consenso, nei casi previsti dal Codice (in particolare, esercizio di un diritto in sede giudiziaria,

salvaguardia della vita o incolumità fisica; specifici obblighi di legge anche in caso di indagine giudiziaria: art. 26).

7.2. *Datori di lavoro pubblici*

Per quanto riguarda i soggetti pubblici restano fermi i differenti presupposti previsti dal Codice a seconda della natura dei dati, sensibili o meno (*artt. 18-22 e 112*).

In tutti i casi predetti resta impregiudicata la facoltà del lavoratore di opporsi al trattamento per motivi legittimi (*art. 7, comma 4, lett. a), del Codice*).

8. Individuazione dei soggetti preposti

Il datore di lavoro può ritenere utile la designazione (facoltativa), specie in strutture articolate, di uno o più responsabili del trattamento cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità (*art. 29 del Codice*).

Nel caso di eventuali interventi per esigenze di manutenzione del sistema, va posta opportuna cura nel prevenire l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti.

Resta fermo l'obbligo dei soggetti preposti al connesso trattamento dei dati (in particolare, gli incaricati della manutenzione) di svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa.

Resta parimenti ferma la necessità che, nell'individuare regole di condotta dei soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, sia svolta un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni (cfr. Allegato B) al Codice, regola n. 19.6; Parere n. 8/2001 cit., punto 9).

TUTTO CIÒ PREMESSO IL GARANTE

1) prescrive ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. c), del Codice, di adottare la misura necessaria a garanzia degli interessati, nei termini di cui in motivazione, riguardante l'onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori (punto 3.1.), indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli;

2) indica inoltre, ai medesimi datori di lavoro, le seguenti linee guida a garanzia degli interessati, nei termini di cui in motivazione, per ciò che riguarda:

a) l'adozione e la pubblicizzazione di un disciplinare interno (punto 3.2.);

b) l'adozione di misure di tipo organizzativo (punto 5.2.) affinché, segnatamente:

- si proceda ad un'attenta valutazione dell'impatto sui diritti dei lavoratori;
- si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e dell'accesso a Internet;
- si individui quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di impieghi abusivi;

c) l'adozione di misure di tipo tecnologico, e segnatamente:

I. rispetto alla "navigazione" in Internet (punto 5.2., a):

- l'individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa;
- la configurazione di sistemi o l'utilizzo di filtri che prevengano determinate operazioni;
- il trattamento di dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni;
- l'eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza;
- la graduazione dei controlli (punto 6.1.);

II. rispetto all'utilizzo della posta elettronica (punto 5.2., b):

- la messa a disposizione di indirizzi di posta elettronica condivisi tra più lavoratori, eventualmente affiancandoli a quelli individuali;
- l'eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato;
- la messa a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, di apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le "coordinate" di altro soggetto o altre utili modalità di contatto dell'istituzione presso la quale opera il lavoratore assente;
- consentire che, qualora si debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- l'inserzione nei messaggi di un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente;
- la graduazione dei controlli (punto 6.1.);

3) vieta ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. d), del Codice, di effettuare trattamenti di dati personali mediante sistemi *hardware* e *software* che mirano al controllo a distanza di lavoratori (punto 4), svolti in particolare mediante:
a) la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
b) la riproduzione e l'eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
c) la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
d) l'analisi occulta di computer portatili affidati in uso;
4) individua, ai sensi dell'art. 24, comma 1, lett. g), del Codice, nei termini di cui in motivazione (punto 7), i casi nei quali il trattamento dei dati personali di natura non sensibile possono essere effettuati per perseguire un legittimo interesse del datore di lavoro anche senza il consenso degli interessati;
5) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana ai sensi dell'art. 143, comma 2, del Codice.
Roma, 1° marzo 2007
IL PRESIDENTE
Pizzetti
IL RELATORE
Paissan
IL SEGRETARIO GENERALE
Buttarelli

2.5. Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro - 4 ottobre 2011

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Daniele De Paoli, segretario generale;
VISTO il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);
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 il dott. Mauro Paissan;
PREMESSO
1. Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro per soddisfare esigenze organizzative, produttive ovvero per la sicurezza sul lavoro e disciplina di protezione dei dati personali
1.1. Con frequenza crescente sistemi di localizzazione e di comunicazione (anche in tempo reale) della posizione rilevata sono installati a bordo dei veicoli impiegati da datori di lavoro pubblici e privati per soddisfare esigenze organizzative e produttive ovvero per la sicurezza sul lavoro nell'ambito della fornitura di servizi di trasporto di persone o cose nonché per dare esecuzione ad ulteriori prestazioni, con riflessi sulla possibilità di localizzare la posizione dei lavoratori assegnatari dei veicoli medesimi.
I dati relativi all'ubicazione dei veicoli, in quanto (direttamente o indirettamente) associati ai lavoratori, costituiscono però anche informazioni personali riferibili a questi ultimi (art. 4, comma 1, lett. b), del Codice) con la conseguenza che al trattamento di tali informazioni trova applicazione la disciplina contenuta nel Codice. Ciò, anche nel caso in cui i dati di localizzazione del veicolo non siano associati immediatamente dal sistema informativo al nominativo dei lavoratori interessati, atteso che il datore di lavoro, titolare del trattamento, è di regola in condizione di risalire in ogni momento al lavoratore di volta in volta assegnatario di ciascun veicolo (cfr., in proposito, Parere n. 5/2005 del 5 novembre 2005 sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto del Gruppo di lavoro articolo 29 per la protezione dei dati, WP 115, p. 10; v. altresì Parere n. 4/2007 sul concetto di dati personali, WP 136, p. 11).
La disciplina di protezione dei dati personali non trova invece applicazione ove le informazioni concernenti la gestione del parco automezzi (quali quelle relative al consumo di carburante e commisurazione delle distanze percorse dai singoli veicoli, utilizzate di regola al fine di programmare un'efficiente manutenzione) siano trattate senza poter essere in alcun modo ricondotte ai lavoratori.
1.2. In relazione ai trattamenti effettuati mediante tali sistemi nell'ambito dell'esecuzione del rapporto di lavoro per soddisfare esigenze organizzative e produttive ovvero per la sicurezza sul lavoro, il Garante ha adottato nel tempo alcune decisioni, sia nell'ambito di procedimenti di verifica preliminare, sia nell'esercizio della propria attività di controllo (cfr. Provv.ti 18 febbraio 2010, in www.garanteprivacy.it, doc. web n. 1703103; 7 ottobre 2010, doc. web n. 1763071; 7 luglio 2011, docc. web n. 1828371 e 1828354).
Anche altre autorità di controllo europee si sono pronunciate in merito e, da ultimo, il "Gruppo di lavoro articolo 29", nel Parere 13/2011 dedicato alla protezione dei dati relativo ai servizi di geolocalizzazione su dispositivi mobili intelligenti (WP 185, adottato il 16 maggio 2011, p. 15), ha affermato che "il datore di lavoro deve […] evitare il monitoraggio costante [… e che i] dispositivi di tracciamento dei veicoli non sono dispositivi di tracciamento del personale, bensì la loro funzione consiste nel rintracciare o monitorare l'ubicazione dei veicoli sui quali sono installati. I datori di lavoro non dovrebbero considerarli come strumenti per seguire o monitorare il comportamento o gli spostamenti di autisti o di altro personale, ad esempio inviando segnali d'allarme in relazione alla velocità del veicolo". Inoltre, riconoscendo che "il consenso come motivo di legittimazione del trattamento è problematico in un contesto lavorativo, [ha auspicato che], invece di chiedere il consenso, i datori di lavoro devono accertarsi che sia possibile dimostrare la necessità di vigilare sull'esatta ubicazione dei dipendenti per una finalità legittima e valutare tale necessità a fronte dei diritti e delle libertà fondamentali dei dipendenti. Nei casi in cui la necessità può essere adeguatamente giustificata, il fondamento giuridico del trattamento si potrebbe basare sull'interesse legittimo" del titolare del trattamento (art. 7, lett. f, direttiva 95/46/CE).
1.3. Alla luce delle considerazioni svolte, il Garante ritiene quindi opportuno individuare, in termini generali, le condizioni di liceità di tali trattamenti effettuati per soddisfare esigenze organizzative e produttive ovvero per la sicurezza sul lavoro nell'ambito del rapporto di lavoro ed in particolare intende, con il presente provvedimento, dare attuazione, nell'ambito qui considerato, all'istituto del c.d. bilanciamento di interessi

(non diversamente dalla determinazione già adottata in passato nella Del. n. 13 del 1° marzo 2007, "Linee guida del Garante per posta elettronica e internet", con particolare riferimento al punto 7, doc. web n. 1387522) e prescrivere, ai sensi dell'art. 154, comma 1, lett. c), del Codice alcune misure opportune rispetto al trattamento dei dati in questione.

2. Liceità nel trattamento dei dati di localizzazione: bilanciamento di interessi

2.1. In termini generali, il trattamento dei dati personali deve avvenire in modo lecito (art. 11, comma 1, lett. a) del Codice), considerata anche la disciplina di settore (cfr. art. 10 Reg. Ce n. 561/2006 del 15 marzo 2006 relativo all'armonizzazione di alcune disposizioni in materia sociale nel settore dei trasporti su strada e che modifica i regolamenti del Consiglio (CEE) n. 3821/85 e (CE) n. 2135/98 e abroga il regolamento (CEE) n. 3820/85 del Consiglio).

2.2. Con specifico riferimento alla materia considerata nel presente provvedimento, la possibilità di individuare in un dato momento la posizione dei veicoli (e quindi dei lavoratori) mediante sistemi di localizzazione può tuttavia rivelarsi utile per soddisfare esigenze organizzative e produttive ovvero per la sicurezza sul lavoro. Finalità che ben possono ricorrere, ad esempio, in caso di impiego dei sistemi in esame per soddisfare esigenze logistiche (consentendo di impartire tempestive istruzioni al conducente del veicolo oggetto di localizzazione), per elaborare rapporti di guida allo scopo di commisurare il tempo di lavoro del conducente – con la conseguente determinazione della retribuzione dovuta, anche in vista dell'assolvimento degli obblighi legali connessi alla tenuta del libro unico del lavoro previsto dall'art. 6, D.M. 9 luglio 2008 (Modalità di tenuta e conservazione del libro unico del lavoro e disciplina del relativo regime transitorio) – ovvero per commisurare i costi da imputare alla clientela, nonché per assicurare una più efficiente gestione e manutenzione del parco veicoli, con effetti vantaggiosi anche sulla sicurezza sul lavoro e per la sicurezza della collettività.

In tali ipotesi, considerato che la localizzazione dei veicoli può comportare una forma di controllo a distanza dell'attività dei lavoratori, oltre alla disciplina di protezione dei dati personali, deve altresì essere rispettata la disciplina dettata dall'art. 4 della legge 20 maggio 1970, n. 300 (Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e nell'attività sindacale nei luoghi di lavoro e norme sul collocamento) peraltro richiamata dagli artt. 11, comma 1, lett. a) e (espressamente) 114 nonché, per i profili sanzionatori, 171 del Codice (nello stesso senso, oltre alle ricordate decisioni di questa Autorità, v. anche il decreto del Ministero del lavoro e delle politiche sociali, Direzione generale della tutela delle condizioni di lavoro, Divisione IV, 24 giugno 2004, in tema di installazione di impianti di controllo satellitare su autovetture di pronto intervento di un'impresa erogatrice di gas, nonché la risposta a una istanza di interpello del medesimo Ministero, Direzione generale per l'attività ispettiva, prot. n. 25/I/0006585 del 28 novembre 2006, in materia di localizzazione mediante computer palmari assegnati in dotazione a informatori scientifici del farmaco).

2.3. Se sono adottate le garanzie previste dall'art. 4, comma 2, l. n. 300/1970, i datori di lavoro privati e gli enti pubblici economici possono effettuare lecitamente il trattamento dei dati personali (diversi da quelli sensibili) relativi all'ubicazione dei propri dipendenti per soddisfare esigenze organizzative e produttive ovvero per la sicurezza sul lavoro (oltre che sulla base di uno degli altri presupposti di cui all'art. 24 del Codice), anche in assenza del consenso degli interessati, per effetto del presente provvedimento che, in applicazione della disciplina sul c.d. bilanciamento di interessi (art. 24, comma 1, lett. g), del Codice), individua un legittimo interesse al trattamento di tale tipologia di dati. Per tale bilanciamento si è tenuto conto delle garanzie che la l. n. 300/1970 prevede per il controllo a distanza presupponendo non il consenso degli interessati, ma un accordo con le rappresentanze sindacali o, in difetto, l'autorizzazione del competente organo periferico del Ministero del lavoro e delle politiche sociali.

2.4. Per quanto riguarda i soggetti pubblici, salva l'applicazione dell'art. 4, l. n. 300/1970 (cfr. art. 42, d. lg. 30 marzo 2001, n. 165, Norme generali sullo ordinamento del lavoro alle dipendenze delle amministrazioni), restano fermi i differenti presupposti previsti dal Codice a seconda della natura dei dati, sensibili o meno (artt. 18-22 e 112).

3. Principi di pertinenza e non eccedenza

3.1. Per il conseguimento di ciascuna delle finalità legittimamente perseguite dal datore di lavoro titolare del trattamento possono formare oggetto di trattamento, mediante sistemi opportunamente configurati (art. 3 del Codice), solo i dati pertinenti e non eccedenti: tali possono essere, oltre all'ubicazione del veicolo, la distanza percorsa, i tempi di percorrenza, il carburante consumato, nonché la velocità media del veicolo (restando riservata alle competenti autorità la contestazione di eventuali violazioni dei limiti di velocità fissati dal codice della strada).

Nel rispetto del principio di necessità (artt. 3 e 11, comma 1, lett. d), del Codice), la posizione del veicolo di

regola non dovrebbe essere monitorata continuativamente dal titolare del trattamento, ma solo quando ciò si renda necessario per il conseguimento delle finalità legittimamente perseguite.
3.2. Con riguardo all'identificazione dei dati personali che possono essere trattati e alla determinazione degli eventuali tempi di loro conservazione, trova generale applicazione l'art. 3 del Codice secondo cui "i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità".
Anche in base al principio di pertinenza e non eccedenza (art. 11, comma 1. lett. e), del Codice) i tempi di conservazione delle diverse tipologie di dati personali eventualmente trattati devono essere commisurati tenendo conto di ciascuna delle finalità in concreto perseguite.
Così, ad esempio, fermi restando gli obblighi di conservazione previsti dall'art. 14, comma 2, Reg. (CEE) 20 dicembre 1985, n. 3821, il titolare del trattamento che intenda avvalersi del sistema di localizzazione anche per la regolare tenuta del libro unico del lavoro, in conformità all'art. 6, D.M. 9 luglio 2008 (Modalità di tenuta e conservazione del libro unico del lavoro e disciplina del relativo regime transitorio), potrà conservare per cinque anni i dati personali necessari, limitatamente alle informazioni che nello stesso devono essere annotate ai sensi dell'art. 39, d.l. 25 giugno 2008, n. 112 (convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 6 agosto 2008, n. 133), con particolare riferimento ai dati dei lavoratori relativi alle presenze nonché ai tempi di lavoro, anche straordinario, e di riposo (cfr. anche art. 8, d.lg. 19 novembre 2007, n. 234 come modificato dall'art. 40, comma 3, d.l. n. 112/2008 nonché la risposta al quesito n. 20 resa dal Ministero del lavoro, della salute e delle politiche sociali nel Vademecum sul libro unico del lavoro). Diversamente, se i dati di localizzazione sono utilizzati al solo scopo di rendere una determinata prestazione contrattuale, gli stessi devono essere cancellati o resi anonimi una volta che alla stessa è stata data esecuzione.

4. Informativa degli interessati

Tenuto conto delle diverse finalità perseguite, ai lavoratori dovranno essere forniti gli elementi informativi prescritti dall'art. 13 del Codice unitamente a compiuti ragguagli sulla natura dei dati trattati e sulle caratteristiche del sistema – sì che risulti chiaramente che il veicolo è soggetto a localizzazione.
A tal fine, considerato che il Garante, ai sensi dell'art. 154, comma 1, lett. c), del Codice, può altresì prescrivere al titolare del trattamento l'adozione di misure opportune per assicurare che il trattamento sia effettuato nel rispetto dei principi di protezione dei dati personali, i datori di lavoro che si avvalgano di sistemi di localizzazione sui veicoli utilizzati per l'esecuzione di prestazioni lavorative dovranno anche collocare all'interno dei veicoli vetrofanie recanti la dizione "VEICOLO SOTTOPOSTO A LOCALIZZAZIONE" o comunque avvisi ben visibili che segnalino la circostanza della geolocalizzazione del veicolo, anche avvalendosi del modello riportato in fac-simile nell'allegato n. 1 al presente provvedimento.

5. Responsabili e incaricati del trattamento dei dati di localizzazione

5.1. Presso il titolare del trattamento, in conformità all'art. 30 del Codice, i dati relativi alla localizzazione dei veicoli devono essere trattati unicamente dagli incaricati che, in ragione delle mansioni svolte, devono poter accedere a tali informazioni per dare attuazione ai propri compiti (quali il personale incaricato di gestire la logistica, i servizi di magazzino e di manutenzione del parco veicoli, ovvero quello operante nell'ambito della gestione delle risorse umane).
5.2. Considerato che i trattamenti dei dati di localizzazione sono di regola effettuati con l'ausilio di operatori economici che forniscono i servizi di localizzazione del veicolo e di trasmissione della posizione del medesimo e tenuto conto che tali soggetti sono terzi rispetto al titolare del trattamento, questi ultimi devono essere designati responsabili del trattamento ai sensi dell'art. 29 del Codice e i titolari del trattamento sono tenuti ad impartire le necessarie istruzioni in ordine all'utilizzo legittimo dei dati raccolti per le sole finalità previste dall'accordo che regola la fornitura del servizio di localizzazione, determinando altresì le tipologie di dati da trattare nonché le modalità e i tempi della loro eventuale conservazione.
5.3. Resta fermo che:
a. il trattamento dei dati di localizzazione deve formare oggetto di notificazione al Garante (cfr. art. 37, comma 1, lett. a), del Codice);
b. trattamenti di dati di localizzazione non considerati nel presente provvedimento e che possono presentare rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità di interessati diversi dai lavoratori possano essere sottoposti a verifica preliminare ai sensi dell'art. 17, comma 2 del Codice.

TUTTO CIÒ PREMESSO IL GARANTE

1. ai sensi dell'art. 24, comma 1, lett. g), del Codice, per effetto del presente provvedimento ammette il trattamento nei termini descritti in narrativa, in applicazione della disciplina sul c.d. bilanciamento di interessi e senza che sia necessario acquisire il consenso dell'interessato, individuando in capo ai datori di lavoro privati che si avvalgono di sistemi di localizzazione e di comunicazione della posizione rilevata installati a bordo dei veicoli ed impiegati per soddisfare esigenze organizzative, produttive ovvero per la sicurezza sul lavoro un legittimo interesse al trattamento dei dati relativi all'ubicazione dei propri dipendenti, a condizione che sia data attuazione alla previsione di cui all'art. 4, l. n. 300/1970, con il previo accordo con le rappresentanze sindacali o, in difetto, con l'autorizzazione del competente organo periferico del Ministero del lavoro e delle politiche sociali (punto 2.3);
2. ai sensi dell'art. 154, comma 1, lett. c), del Codice, prescrive ai datori di lavoro pubblici e privati che si avvalgono di sistemi di localizzazione e di comunicazione della posizione rilevata installati a bordo dei veicoli ed impiegati per soddisfare esigenze organizzative, produttive ovvero per la sicurezza sul lavoro:
a. quale misura necessaria, nel rispetto del principio di necessità, che la posizione del veicolo non sia di regola monitorata continuativamente dal titolare del trattamento, ma solo quando ciò si renda necessario per il conseguimento delle finalità legittimamente perseguite (punto 3.1);
b. quale misura necessaria, in base al principio di pertinenza e non eccedenza, che i tempi di conservazione delle diverse tipologie di dati personali eventualmente trattati siano commisurati tenendo conto di ciascuna delle finalità in concreto perseguite (punto 3.2);
c. quale misura necessaria, la designazione quali responsabili del trattamento ai sensi dell'art. 29 del Codice degli operatori economici che forniscono i servizi di localizzazione del veicolo e di trasmissione della posizione del medesimo, impartendo loro le necessarie istruzioni in ordine all'utilizzo legittimo dei dati raccolti per le sole finalità previste dall'accordo che regola la fornitura del servizio di localizzazione, con la determinazione delle tipologie di dati da trattare nonché delle modalità e dei tempi della loro eventuale conservazione (punto 5.2);
d. quale misura opportuna, un modello semplificato di informativa, quale quello individuato nell'allegato 1, utilizzabile alle condizioni indicate in motivazione, al fine di rendere noto agli interessati il trattamento effettuato mediante il sistema di localizzazione del veicolo (punto 4).
Roma, 4 ottobre 2011

IL PRESIDENTE
Pizzetti
IL RELATORE
Paissan
IL SEGRETARIO GENERALE
De Paoli

2.6. Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone. Verifica preliminare richiesta da Ericsson Telecomunicazioni s.p.a. - 11 settembre 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.lg. 30 giugno 2003, n. 196, di seguito "Codice") ;
ESAMINATA la richiesta di verifica preliminare presentata da Ericsson Telecomunicazioni s.p.a. ai sensi dell'art. 17 del Codice;
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 prof.ssa Licia Califano;

PREMESSO

1. Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone.

1.1. Ericsson Telecomunicazioni s.p.a. (di seguito: la società) ha presentato il 1° aprile 2014 una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, in relazione al trattamento di dati personali connesso all'attivazione di una nuova funzionalità di localizzazione di dispositivi smartphone che verrebbero forniti in dotazione dalla società ai propri dipendenti nell'ambito di un sistema di Work Force Management (WFM) già esistente.

Tali dispositivi, dotati di GPS (Global Positioning System) capace di effettuare la localizzazione geografica "con un'accuratezza di 31 m circa", sarebbero in grado di comunicare al sistema WFM la propria posizione con una periodicità temporale prestabilita pari a 15 minuti. Il dato relativo alla geolocalizzazione così raccolto non sarebbe acquisito in modo permanente dal sistema bensì automaticamente cancellato in modo tale che "sarà disponibile solo l'ultimo dato di localizzazione pervenuto, ovvero la nuova posizione rilevata annulla e sostituisce la precedente" (cfr. comunicazione dell'1.4.2014, par. 1, "Chiarimenti sul funzionamento del sistema di geo-localizzazione"). Secondo quanto dichiarato dalla società, pertanto, tramite l'attivazione di tale funzionalità "non viene mantenuto e non si ha a disposizione il tracciamento del percorso. Il sistema mantiene solo i dati master (ad esempio siti, attrezzature, ecc) mentre i dati transazionali (ad esempio dettaglio dei WO) vengono eliminati dal sistema dopo 16 giorni dalla chiusura. Dopo questo periodo di tempo i dati vengono distrutti" (cfr. comunicazione cit., par. 4, "Storicizzazione delle informazioni").

I dati personali complessivamente trattati dal sistema sarebbero: "cognome, nome, Service Area, Skill tecnico (es. radio, transmission, power, ecc), Home Base (ovvero dove il tecnico prende servizio), Attività svolta, dato dell'ultima localizzazione rilevato tramite funzionalità GPS dell'applicazione" (cfr. comunicazione cit., par. 4, "Trattamento Dati e Principio di base").

Gli scopi che la società intende perseguire (cfr. comunicazione cit., par. 2, "Specifica delle esigenze che impongono l'introduzione del sistema di geo-localizzazione") attraverso l'attivazione della menzionata funzionalità di localizzazione sono:

a. disporre l'intervento di propri tecnici in modo tale da consentire il rispetto dei termini contrattuali stipulati con i clienti, che risultano "particolarmente stringenti in quanto l'attività di manutenzione condotta [dalla società] deve supportare la continuità del servizio pubblico offerto dal cliente, inclusa la pronta gestione dei ripristini in caso di emergenze non ultime quelle generate da disastri naturali/ambientali";

b. intervenire (più) rapidamente con personale specializzato in caso di calamità naturali;

c. migliorare il coordinamento operativo dei "circa 330 tecnici dislocati sul territorio", in modo tale da poter "indirizzare prontamente i tecnici in servizio con le idonee competenze più prossimi al sito oggetto dell'intervento richiesto";

d. incrementare la sicurezza dei tecnici stessi in caso di incidenti o situazioni di difficoltà.

Ciò posto, "nessun utilizzo dei dati potrà avvenire per finalità diverse da quelle dichiarate, come ad esempio per scopi disciplinari".

Precisato pertanto che la funzione di geolocalizzazione "sarà finalizzata alla sola gestione operativa delle attività di manutenzione", secondo quanto dichiarato, non sono conseguentemente previste forme di interazione "con altri sistemi aziendali quali, a mero titolo esemplificativo, quelli deputati al time reporting" (cfr. comunicazione cit., par. 5, "Interazione tra il sistema di geo-localizzazione ed ulteriori sistemi/strumenti elettronici aziendali").

La società ha inoltre dichiarato che fornirà ai tecnici specifiche istruzioni operative in ordine alla attivazione e disattivazione della "applicazione GPS […] per rendere possibile l'utilizzo alternativo dello «smart phone» durante l'orario di lavoro (con tracking GPS) e fuori orario di lavoro (senza GPS tracking)"; sarà inoltre data indicazione di "mantenere tale funzionalità attiva durante l'orario di lavoro fatti salvi gli usuali casi di interruzione previsti dal […] rapporto di lavoro, quali ad esempio il proprio turno mensa" (cfr. comunicazione cit., par. 4, "Attivazione e Disattivazione dell'applicazione"). La società ha inoltre dichiarato che provvederà a fornire agli interessati un'apposita informativa relativa alle caratteristiche del trattamento, anche attraverso la

predisposizione di uno specifico "protocollo" (cfr. comunicazione cit., par. 7, "Informativa degli interessati").
Per quanto riguarda, infine, il rispetto della disciplina vigente in materia di controlli a distanza dei dipendenti la società si è impegnata "ad adottare le garanzie previste dall'art. 4 comma 2 della L. n. 300 del 1970 e quindi a raggiungere un accordo con le OO.SS. o, in difetto, ad acquisire l'autorizzazione del competente organo del Ministero del Lavoro e delle politiche sociali" (cfr. comunicazione cit., par. 6, "Liceità del trattamento e bilanciamento di interessi").
1.2. A seguito di una richiesta di chiarimenti ed integrazioni formulata dall'Autorità (in data 7.5.2014), la società ha successivamente precisato che:

a. il trattamento di dati personali relativi alla localizzazione dei dispostivi smartphone avviene mediante accesso dell'utente "all'applicazione «WFM Click Mobile Touch» attraverso un'autenticazione basata su userid e password"; la password deve essere modificata dopo il primo accesso rispettando determinati requisiti minimi di sicurezza (cfr. nota del 20.5.2014, p. 1);

b. la possibilità tecnica di accedere alla posizione geografica del dispositivo in un momento dato al di fuori dell'intervallo temporale prestabilito (15 minuti) "non sussiste" (cfr. nota cit., p. 5);

c. i dati c.d. transazionali, "di natura operativa e [che] contengono le informazioni relative agli ordinativi di lavoro […] sono memorizzati localmente e quindi sono presenti solo sul dispositivo mobile. [...] L'operazione di cancellazione compiuta dall'utente tramite la funzione «clear stored data» determina la rimozione dei suddetti dati dal dispositivo mobile" (cfr. nota cit., p. 5);

d. posto che "al termine dell'orario di lavoro ovvero in occasione delle consentite interruzioni dell'attività lavorativa (es. pausa pranzo) il dipendente può disattivare manualmente l'applicazione" in ogni caso, anche qualora il dipendente non provvedesse alla disattivazione manuale "l'applicazione si disattiverà automaticamente dopo 120 minuti di inattività" (cfr. nota cit., p. 5);

e. in caso di furto o smarrimento del dispositivo si prevede "l'immediato blocco dell'utenza mobile attraverso la denuncia alle AA.GG. e la richiesta di blocco all'operatore telefonico" (cfr. nota cit., p. 6);

f. quanto ai tempi di conservazione "il sistema WFM, relativamente ai dati di localizzazione, mantiene solo la località di partenza del FT e l'ultima posizione conosciuta. Nessuna informazione storica relativa alla localizzazione è mantenuta nel Sistema" (cfr. All. nota cit., punto 2.4 "Conservazione dei dati").

1.3 Con successiva nota del 30.6.2014, rispondendo ad ulteriori richieste dell'Autorità, la società ha infine specificato che:

a. "le informazioni che saranno scambiate tra il tecnico di campo ed il sistema WFM sono esclusivamente finalizzate all'assegnazione e gestione dei work order, non sono previste alla data interazioni con altre informazioni presenti sul dispositivo mobile (es. dati di traffico telefonico, sms, posta elettronica o altro)"; la società, in proposito, intende impartire ai dipendenti apposite istruzioni relative alla necessaria adozione di "misure organizzative procedurali da osservare per evitare trattamenti di dati non attinenti ai work order quali ad esempio: non riportare in eventuali aree di commento disponibili con gli SMS o email scambiate con il WFM riferimenti alla vita privata dei singoli, disattivare l'applicazione di geolocalizzazione presente sullo smart-phone al di fuori degli orari di lavoro" (cfr. nota 30.6.2014, p. 2);

b. il sistema consente (così rettificando quanto affermato in precedenti comunicazioni all'Autorità) la visualizzazione in tempo reale del dato di localizzazione benché "solo ed esclusivamente [in relazione] ad esigenze di assegnazione e gestione dei work order ai tecnici di campo, per soddisfare i requisiti dei servizi operati sulle reti dei Clienti operatori di telecomunicazioni" (cfr. nota cit., p. 3).

2. Trattamento di dati personali dei dipendenti attraverso la localizzazione di dispositivi smartphone.

Il trattamento di dati personali che la società ha sottoposto a verifica preliminare è connesso all'attivazione di un'applicazione (Click Schedule) del sistema di gestione della mano d'opera già in uso (WFM), in grado di interagire – attraverso l'applicazione ClickMobile-WAP – con i dispositivi mobili geolocalizzati (smartphone) posti in dotazione ai tecnici che effettuano interventi sul campo.
Tale trattamento, rispetto alle ipotesi prese in considerazione dall'Autorità nel provvedimento di carattere generale n. 370 del 4 ottobre 2011, relativo all'utilizzo di sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro [in www.garanteprivacy.it, doc. web n. 1850581], presenta caratteristiche particolari proprio in considerazione dell'utilizzo di un dispositivo smartphone messo a disposizione dei dipendenti allo scopo di procedere alla raccolta dei dati di localizzazione. Tali dispositivi, in considerazione delle normali potenzialità d'uso nonché in ragione dell'utilizzo oramai comune degli stessi, possono essere agevolmente impiegati anche per finalità diverse da quelle lavorative. Tali ulteriori (e comuni) modalità di impiego sono d'altra parte (ragionevolmente) consentite dalla società (cfr. punto 1.1 laddove ci si riferisce all'"l'utilizzo alternativo dello «smart phone» durante […] e fuori [l']orario di lavoro"). Inoltre lo smartphone è, per le proprie caratteristiche, destinato inevitabilmente a "seguire" la persona che lo possiede, indipendentemente dalla distinzione tra tempo di lavoro e tempo di non lavoro.
Il descritto trattamento pertanto presenta rischi specifici per la libertà (es. di circolazione e di comunicazione), i diritti (v. artt. 10, D.Lg. 276/2003 e 8, l. n. 300/1970) e la dignità del dipendente e richiede una specifica ed attenta valutazione da parte dell'Autorità.

3. Liceità del trattamento dei dati di localizzazione: bilanciamento di interessi.

3.1 Le finalità del trattamento, così come rappresentate dalla società, risultano lecite. La funzionalità di localizzazione geografica consente infatti di ottimizzare la gestione ed il coordinamento degli interventi effettuati dai tecnici sul campo, incrementandone la tempestività a fronte delle richieste dei clienti, soprattutto in caso di emergenze e/o calamità naturali. La localizzazione consente altresì di rafforzare le condizioni di sicurezza del lavoro effettuato dai tecnici stessi, permettendo l'invio mirato di eventuali soccorsi soprattutto in aree remote o non facilmente raggiungibili e comunque di supportare più rapidamente i lavoratori in caso di difficoltà.
I trattamenti di dati personali, pertanto, sarebbero effettuati nell'ambito del rapporto di lavoro per soddisfare esigenze organizzative e produttive ovvero per la sicurezza del lavoro, coerentemente con quanto stabilito dalla disciplina di settore in materia di controllo a distanza dei dipendenti (cfr. artt. 11, comma 1, lett. a) e 114 del Codice e 4, legge n. 300/1970). In proposito la società ha dichiarato che le informazioni riferibili ai possessori dei dispositivi saranno utilizzate per finalità non riconducibili a quelle di controllo degli stessi, tanto che nessun "utilizzo dei dati potrà avvenire per finalità diverse da quelle dichiarate, come ad esempio per scopi disciplinari" (comunicazione 1.4.2014, par. 2.3). Il menzionato sistema, sempre in base a quanto sostenuto, non potrà interagire con altri sistemi aziendali, compresi quelli volti a valutare il corretto adempimento della prestazione lavorativa.
3.2 Pertanto, considerato anche che la società ha dichiarato che procederà ad attivare le procedure previste dall'art. 4, comma 2, della legge n. 300/1970 visto che la localizzazione di dispostivi associati a dipendenti identificati può comportare il controllo a distanza dell'attività degli stessi, il menzionato trattamento potrà essere lecitamente effettuato anche senza il consenso degli interessati, per effetto del presente provvedimento che, in applicazione della disciplina sul c.d. bilanciamento di interessi (art. 24, comma 1, lett. g) del Codice), individua un legittimo interesse al trattamento di tale tipologia di dati (diversi da quelli sensibili) in relazione alle finalità rappresentate.

4. Principi di pertinenza e non eccedenza del trattamento.

4.1 Il trattamento dei dati di localizzazione per le finalità sopra indicate appare altresì nel complesso conforme ai principi di necessità nonché di pertinenza e non eccedenza (artt. 3 e 11, comma 1, lett. d), del Codice), alla luce delle circostanze rappresentate nell'istanza e in particolare considerato che:

a. non si effettuerebbe (di regola) la rilevazione continuativa di dati relativi alla localizzazione geografica dei tecnici bensì con periodizzazione temporale pari a 15 minuti;

b. il sistema sarebbe configurato in modo tale da memorizzare solo l'ultima informazione relativa alla localizzazione del dispositivo al termine di una determinata sessione di lavoro, procedendo a cancellare automaticamente la rilevazione precedente.

4.2 Tuttavia, posto che la società ha dichiarato che il sistema è configurato in modo tale da consentire agli utenti autorizzati all'accesso la visualizzazione in tempo reale dei dati di localizzazione, anche al di fuori della periodizzazione stabilita in via ordinaria (cfr. punto 1.3, lett. b.), l'Autorità ritiene di prescrivere, come misura posta a tutela dei diritti degli interessati, che tale eventuale trattamento di dati in tempo reale avvenga solo in presenza di specifiche esigenze (ad es. legate al verificarsi di situazioni di emergenza e/o di pericolo per il dipendente), individuate all'interno di appositi protocolli che individuino anche i soggetti legittimati ad accedere con tale modalità al sistema.

5. Misure ed accorgimenti posti a tutela dei diritti degli interessati.

5.1. Considerate le menzionate potenzialità dei dispostivi smartphone e segnatamente la possibilità di raccogliere per loro tramite, anche accidentalmente, informazioni relative alla vita privata del dipendente, la società dovrà:

a. adottare specifiche misure idonee a garantire che le informazioni presenti sul dispositivo mobile visibili o utilizzabili dall'applicazione installata siano riferibili esclusivamente a dati di geolocalizzazione nonché ad impedire l'eventuale trattamento di dati ultronei (es. dati relativi al traffico telefonico, agli sms, alla posta elettronica o altro);

b. configurare il sistema in modo tale che sul dispositivo sia posizionata un'icona che indichi che la funzionalità di localizzazione è attiva; l'icona dovrà essere sempre chiaramente visibile sullo schermo del dispositivo, anche quando l'applicazione Click Mobile Touch lavora in background.

5.2. In applicazione del principio di correttezza (art. 11, comma 1, lett. a) del Codice) i trattamenti in esame devono essere resi noti agli interessati, i quali devono essere posti nella condizione di conoscere chiaramente finalità e modalità del trattamento. A tal fine la società dovrà fornire ai dipendenti una puntuale informativa, comprensiva di tutti gli elementi contenuti nell'art. 13 del Codice.

5.3 Si ritiene inoltre opportuno che tra le istruzioni da fornire ai dipendenti relativamente all'utilizzo del dispositivo, si raccomandi di effettuare periodicamente la pulizia dei dati memorizzati localmente attraverso l'attivazione della funzione "clear stored data" (cfr. punto 1.2, lett. c.), fatte salve eventuali esigenze di conservazione da parte del lavoratore .

6. Adempimenti ulteriori e misure di sicurezza.

6.1. Resta fermo che:

a. considerato che il dispositivo che si intende installare comporta il trattamento di dati relativi alla localizzazione, la società è tenuta ad effettuare la notificazione ai sensi dell'art. 37, comma 1, lett. a), del Codice;

b. la società dovrà attenersi, in quanto applicabili, alle prescrizioni ed alle raccomandazioni contenute nel provvedimento n. 13 del 1° marzo 2007 "Linee guida per posta elettronica e internet" (doc. web n. 1387522) (es. in caso di trattamenti effettuati in occasione della predisposizione di idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati; a seguito della riconsegna del dispositivo per interventi di manutenzione o a seguito della cessazione del rapporto di lavoro);

c. gli interessati potranno esercitare i diritti di cui agli artt. 7 ss. del Codice in relazione ai dati personali che li riguardano rilevati mediante il dispositivo in esame;

d. dovranno essere adottate le misure di sicurezza previste dagli artt. 31 ss. del Codice al fine di preservare l'integrità dei dati trattati e prevenire l'accesso agli stessi da parte di soggetti non autorizzati.

TUTTO CIÒ PREMESSO IL GARANTE

1. ai sensi dell'art. 17 del Codice, preso atto della richiesta di verifica preliminare presentata da Ericsson Telecomunicazioni s.p.a. in relazione ai trattamenti da effettuare mediante l'attivazione di una funzionalità di localizzazione di dispositivi mobili smartphone forniti in dotazione ai propri dipendenti per finalità organizzative, produttive e connesse alla sicurezza

del lavoro, ritiene ammissibile il trattamento da effettuarsi nei termini di cui in motivazione, fermo restando che:

a. la società, quali misure necessarie, dovrà:

i. adottare specifiche misure idonee a garantire che le informazioni presenti sul dispositivo mobile visibili o utilizzabili dall'applicazione installata siano riferibili esclusivamente a dati di geolocalizzazione nonché ad impedire l'eventuale trattamento di dati ultronei (es. dati relativi al traffico telefonico, agli sms, alla posta elettronica o altro);

ii. configurare il sistema in modo tale che sul dispositivo sia posizionata un'icona che indichi che la funzionalità di localizzazione è attiva; l'icona dovrà essere sempre chiaramente visibile sullo schermo del dispositivo, anche quando l'applicazione Click Mobile Touch lavora in background (punto 5.1, lett. b.);

iii. consentire l'eventuale trattamento dei dati in tempo reale solo in presenza di specifiche esigenze (ad es. legate al verificarsi di situazioni di emergenza e/o di pericolo per il dipendente), individuate all'interno di appositi protocolli (punto 4.2);

iv. consentire l'accesso ai dati trattati ai soli incaricati della società che, in ragione delle mansioni svolte o degli incarichi affidati, possono prenderne legittimamente conoscenza;

b. la società, quale misura opportuna, dovrà raccomandare ai dipendenti di effettuare periodicamente la pulizia dei dati memorizzati localmente attraverso l'attivazione della funzione "clear stored data", fatte salve eventuali esigenze di conservazione da parte del lavoratore (punto 5.3);

c. la società dovrà notificare al Garante il trattamento dei dati relativi alla localizzazione (punto 6.1, lett. b);

d. ai dipendenti della società, unitamente agli elementi previsti dall'art. 13 del Codice, dovranno essere fornite informazioni chiare e complete sulla natura dei dati trattati e sulle caratteristiche del dispositivo, tenuto conto delle finalità mediante lo stesso perseguite (punto 5.2); i dipendenti dovranno altresì essere compiutamente informati sulle ipotesi in cui è consentita la disattivazione della funzione di localizzazione nel corso dell'orario di lavoro nonché circa le eventuali conseguenze nel caso in cui la disattivazione avvenga con modalità non consentite;

e. la società dovrà attenersi, in quanto applicabili, alle prescrizioni ed alle raccomandazioni contenute nel provvedimento n. 13 del 1° marzo 2007 "Linee guida per posta elettronica e internet" (doc. web n. 1387522) (es. in caso di trattamenti effettuati in occasione della predisposizione di idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati; a seguito della riconsegna del dispositivo per interventi di manutenzione o a seguito della cessazione del rapporto di lavoro);

f. gli interessati potranno esercitare i diritti di cui agli artt. 7 ss. del Codice in relazione ai dati personali che li riguardano rilevati mediante il dispositivo in esame;

g. dovranno essere adottate le misure di sicurezza previste dagli artt. 31 ss. del Codice al fine di preservare l'integrità dei dati trattati e prevenire l'accesso agli stessi da parte di soggetti non autorizzati.

2. ai sensi dell'art. 24, comma 1, lett. g) del Codice, in applicazione della disciplina sul c.d. bilanciamento di interessi, per effetto del presente provvedimento il trattamento descritto può essere effettuato senza che sia necessario acquisire il consenso degli interessati, individuando in capo ad Ericsson Telecomunicazioni s.p.a., in relazione all'installazione di un sistema di localizzazione degli smartphone dati in dotazione ai dipendenti, un legittimo interesse volto a soddisfare esigenze organizzative, produttive e legate alla sicurezza del lavoro previa attivazione delle procedure previste dall'art. 4, comma 2, della legge n. 300/1970 (punto 3.2).

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, 11 settembre 2014

IL PRESIDENTE
Soro
IL RELATORE
Califano
IL SEGRETARIO GENERALE
Busia

2.7. Sistemi di localizzazione e videosorveglianza. Utilizzo dei dati per fini disciplinari e tutela dei lavoratori - 2 ottobre 2014

Registro dei provvedimenti
n. 434 del 2 ottobre 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;
ESAMINATA la documentazione in atti;
VISTO il d.lg. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, di seguito "Codice");
VISTO il provvedimento generale adottato dal Garante l'8 aprile 2010, in materia di trattamento di dati personali effettuato tramite sistemi di videosorveglianza (pubblicato sulla Gazzetta Ufficiale n. 99 del 29 aprile 2010 e in www.garanteprivacy.it, doc. web n. 1712680);
VISTI i verbali degli accertamenti ispettivi effettuati, a seguito di una segnalazione al Garante, il 24 e 25 settembre 2013 dal Nucleo Speciale Privacy della Guardia di Finanza presso la sede di A.M.A.CO. s.p.a. di Cosenza (di seguito, la società), dai quali, in relazione all'installazione di un impianto di videosorveglianza, è emerso che:
- il sistema è composto da undici telecamere poste all'esterno degli edifici della società e in corrispondenza degli accessi, e da una telecamera collocata all'interno dell'edificio principale che visualizza "l'ingresso e parte dell'atrio, senza inquadrare direttamente il rilevatore per la lettura dei badge ivi presente", nonché di un server dove le registrazioni delle immagini (posto che, secondo quanto dichiarato, non sarebbe prevista alcuna registrazione audio) sono conservate per 72 ore (cfr. verbale 24.9.2013, p. 3 e 4);
- l'adozione (e la successiva implementazione) del menzionato sistema, secondo quanto rappresentato dal titolare del trattamento, si è resa necessaria allo scopo di "tutelare il patrimonio aziendale ed i beni di terzi (ad es. autobus del Comune con i quali si svolge il servizio di scuolabus e veicoli rimossi che si trovano parcheggiati all'interno della struttura), nonché per finalità di sicurezza, dato che è presente in struttura un impianto di rifornimento del metano ed un impianto di rifornimento di gasolio", anche a seguito del verificarsi, in passato, di furti ed accessi non autorizzati (cfr. verbale cit., p. 3 e 4);

- la presenza delle telecamere, come accertato in sede di sopralluogo, "è adeguatamente segnalata da cartelli di vario tipo" (cfr. verbale cit., p. 3);
- la Direzione Territoriale del Lavoro di Cosenza, a seguito dell'ispezione effettuata il 2.5.2013 presso i locali della società e della successiva verifica dell'adempimento delle prescrizioni nell'occasione impartite, in data 4.9.2013 ha autorizzato, ai sensi dell'art. 4, comma 2, legge n. 300/1970, l'installazione del sistema di videosorveglianza (cfr. All. 2 verbale cit.);
- secondo quanto dichiarato dal rappresentate della società "il sistema è stato utilizzato una sola volta per fare contestazioni disciplinari ad un dipendente, dirigente sindacale. In quella circostanza, fu rilevato lo spostamento di due telecamere e, ipotizzando danneggiamenti, l'azienda si rivolse ai Carabinieri, con i quali furono viste le registrazioni e fu riscontrato che il dipendente aveva manomesso (spostate verso l'alto) le telecamere, pur senza danneggiarle, ed era entrato con la propria autovettura in un'area vietata" (cfr. verbale cit., p. 3 e 4);
VISTO che a seguito dei menzionati accertamenti ispettivi, in relazione all'installazione di un sistema di localizzazione dei veicoli, è emerso che:
- il sistema prevede la localizzazione di 44 (su 57) veicoli adibiti al trasporto di persone dotati, allo scopo, di rilevatore GPS/GPRS (cfr. verbale 25.9.2013, p. 2);

- posto che il predetto sistema "è concretamente utilizzato per una ridottissima parte delle sue potenzialità", le informazioni allo stato rilevate sono: posizione geografica del veicolo, apertura porte, azionamento pedana disabili, superamento della velocità massima consentita (cfr. verbale cit., p. 3);
- tali informazioni sono "associate a ciascun veicolo […], individuato con l'identificativo assegnato dal sistema stesso. Solo attraverso l'eventuale confronto con il foglio di servizio […] e con la verifica dell'assegnazione giornaliera del veicolo, è possibile associare al singolo dipendente le informazioni riferite ad una determinata vettura" (cfr. verbale cit., p. 3);
- in sede di sopralluogo è stato accertato che "il segnale che determina la localizzazione dei veicoli viene rilevato solo al verificarsi degli eventi configurati", ossia: "accensione", "spegnimento" [funzioni di base], "pedana fuori", "porta aperta" e "velocità superiore a 50Km/h" [funzioni avanzate] (cfr. verbale cit., p. 2);
- nel corso del sopralluogo è stato altresì accertato che "i dati rilevati […] non vengono cancellati e restano memorizzati nel sistema, dal quale è [anche] emerso che il «Diario di bordo» meno recente in relazione al veicolo […] risale al 03.01.2011" (cfr. verbale cit., p. 2);
- su 44 veicoli geolocalizzati "solo per n. 36 è possibile ricostruire il «Diario di bordo», ovvero gli spostamenti rilevati (attraverso i predetti parametri), in quanto i restanti n. 8, non dotati di impianto elettrico monocavo, sono in grado di far rilevare solo i segnali emessi per «accensione» e «spegnimento» del veicolo" (cfr. verbale cit., p. 2);
- gli autisti dei veicoli hanno anche l'obbligo "di compilare, per ciascun turno effettuato, un foglio di marcia, contenente, per ciascuna corsa, località ed orari di partenza e di arrivo ed eventuali anomalie riscontrate (corsa in ritardo; corsa limitata; ecc.). Tale foglio di marcia, così come il foglio di servizio, viene conservato per cinque anni in ottemperanza alla disciplina vigente" (cfr. verbale cit., p. 3);
- secondo quanto dichiarato dalla società in relazione ai tempi di conservazione dei dati, "il sistema non è predisposto per cancellare i dati raccolti, posto che l'azienda, in particolare per quanto riguarda i dati storici, li utilizza solo per finalità tecnico-statistiche […] dunque senza associarli ai nominativi dei singoli dipendenti" (cfr. verbale cit., p. 3);
- con riferimento alle finalità perseguite attraverso il trattamento dei dati relativi alla localizzazione dei veicoli la società ha rappresentato che queste consistono nella: gestione dei reclami; definizione dei tempi di percorrenza dei veicoli al fine di realizzare il programma di esercizio; miglioramento della qualità del servizio attraverso l'elaborazione di informazioni tecnico-statistiche; verifica dello stato di efficienza dei veicoli; nonché l'effettuazione di "verifiche relative ad eventuali denunce di sinistri occorsi ai veicoli, dai quali dovesse scaturire la necessità di consultare i dati registrati sul

Diario di bordo [sebbene f]inora questa eventualità non si [sia] mai verificata" (cfr. verbale cit., p. 3);
- per quanto riguarda, in particolare, l'attività di gestione dei reclami, la società ha specificato che al momento della ricezione di una lamentela sul servizio, per prima cosa viene effettuata una verifica sul foglio di marcia all'interno del quale l'autista ha l'obbligo di annotare eventuali irregolarità di servizio occorse. "Solo nel caso in cui sul foglio di marcia [...] non risultasse alcuna irregolarità riconducibile all'oggetto del reclamo, l'azienda può ritenere opportuno consultare i dati del sistema ed, eventualmente, avviare un procedimento disciplinare"; la società ha comunque tenuto a precisare che "la consultazione dei dati relativi alla geolocalizzazione, nella gran parte dei casi, non [ha] comportato l'adozione di provvedimenti disciplinari" (cfr. verbale cit., p. 4);
- in definitiva "posto che la finalità principale è quella di fornire adeguata risposta ai reclami dell'utenza – anche alla luce del regolamento per la gestione delle segnalazioni degli utenti, che ci impone di rispondere agli stessi entro trenta giorni, nonché dei criteri in base ai quali poter conseguire la certificazione di qualità del servizio ISO 9000/2008 – il controllo è effettuato solo a posteriori. Non c'è controllo in tempo reale né monitoraggio continuo [né], pertanto, […] controllo a distanza dei lavoratori" (cfr. verbale cit., p. 3 e 4);
- per quanto riguarda l'obbligo di informare i dipendenti ai sensi dell'art. 13 del Codice, la società ha dichiarato di non aver disposto l'affissione di vetrofanie sui singoli automezzi dato che "tutti gli autisti sono stati compiutamente informati, in occasione dei corsi di formazione tenutisi in occasione dell'arrivo dei veicoli a metano […], che sono quelli dotati di rilevatore per la geolocalizzazione, e in occasione dei corsi tenutisi per l'assunzione di nuovi autisti. Peraltro, questi veicoli sono riconoscibili dagli autisti in quanto presentano alcune caratteristiche peculiari, quali, ad esempio: presenza del computer di bordo, colore rosso anziché arancione e alimentazione a metano anziché a gasolio" (cfr. verbale cit., p. 4);
- i dati raccolti tramite il menzionato sistema "sono accessibili solo mediante una procedura di autenticazione e sono custoditi nel pc/server e sui supporti che si trovano nella disponibilità dello specialista tecnico dell'azienda" (cfr. verbale cit., p. 4);
- la società non ha provveduto ad effettuare la notificazione "in quanto non era al corrente dell'esistenza di tale obbligo" (cfr. verbale cit., p. 4);
- per quanto riguarda, infine, la conformità alla disciplina di settore in materia di controllo a distanza dei lavoratori in relazione all'adozione del sistema di localizzazione "fino ad ora non sono state avviate le procedure previste dall'art. 4, c. 2, della legge 300/1970 perché non si riteneva di essere tenuti ad ottemperarle" (cfr. verbale cit., p. 5);
VISTA la nota dell'8.10.2013 con la quale la società ha comunicato di aver effettuato nella medesima data la notificazione al Garante ai sensi dell'art. 37, co. 1, lett. a) del Codice;
VISTO l'art. 10, comma 2, dello schema di contratto per l'affidamento dei servizi di trasporto pubblico locale su gomma, approvato con deliberazione della giunta della regione Calabria n. 173 del 20.5.2013, in base al quale la società affidataria dei servizi "si dota di un sistema di certificazione della percorrenza, che sarà necessariamente ed inderogabilmente posto in funzione dal 1° luglio 2013, in grado anche di conoscere la posizione di ciascun mezzo in tempo reale";
VISTO che, a seguito degli accertamenti, la società è risultata essere titolare dei trattamenti di dati personali effettuati ai sensi dell'art. 28 del Codice;
RILEVATO che in termini generali il trattamento di dati personali dei dipendenti effettuato dalla società attraverso il sistema di videosorveglianza, allo stato, anche in considerazione dell'adempimento delle prescrizioni impartite dalla competente Direzione Territoriale del Lavoro, non si pone in contrasto con la disciplina di protezione dei dati personali né con il richiamato provvedimento generale dell'8.4.2010;
RITENUTO, tuttavia, che nel caso di specie i dati personali dei dipendenti sono trattati attraverso il sistema di videosorveglianza per finalità di tutela dei beni aziendali e di terzi nonché per finalità di sicurezza e che pertanto eventuali operazioni di trattamento effettuate allo scopo ulteriore di contestare illeciti disciplinari ai dipendenti non siano conformi al principio di finalità del

trattamento (cfr. art. 11, comma 1, lett. b) del Codice); ritenuto che tali ulteriori trattamenti non siano altresì conformi alla disciplina posta in materia di controllo a distanza dei dipendenti, posto che, secondo quanto chiarito dal Garante, "non devono essere effettuate riprese al fine di verificare […] la correttezza nell'esecuzione della prestazione lavorativa" (cfr. provvedimento 8.4.2010 cit., punto 4.1);
VISTO che attraverso il descritto sistema di localizzazione la società effettua un trattamento di dati personali attraverso l'eventuale confronto con il foglio di servizio e la verifica dell'assegnazione del veicolo aziendale al dipendente;
VISTO il provvedimento n. 370 adottato dal Garante il 4 ottobre 2011, in materia di sistemi di localizzazione di veicoli nell'ambito del rapporto di lavoro (pubblicato in www.garanteprivacy.it, doc. web n. 1850581) e in particolare il punto 2, dove si chiarisce che i titolari del trattamento possono effettuare lecitamente il trattamento al fine di soddisfare esigenze organizzative e produttive ovvero per la sicurezza sul lavoro, anche in assenza del consenso degli interessati, purché venga osservata la disciplina di settore in materia di controlli a distanza dei dipendenti (artt. 114 del Codice e 4, l. 20.5.1970, n. 300);

RITENUTO pertanto che, con riferimento al principio di liceità (v. art. 11, comma 1, lett. a) e 114 del Codice), i trattamenti effettuati dalla società attraverso il sistema di localizzazione al dichiarato fine di migliorare la qualità del servizio, di gestire i reclami degli utenti (anche verificandone l'attendibilità) nonché di ottemperare a quanto richiesto dalla regione Calabria in sede di affidamento del servizio, consentono altresì di effettuare il controllo a distanza dell'attività dei dipendenti che prestano servizio a bordo dei veicoli aziendali; in base a quanto previsto dalla specifica disciplina di settore (art. 4, comma 2, l. 20.5.1970, n. 300), devono dunque essere attivate le procedure di garanzia ivi previste (accordo con le rappresentanze sindacali aziendali oppure, in difetto di accordo, autorizzazione rilasciata dalla competente Direzione Territoriale del Lavoro);
RITENUTO altresì che nel caso di specie i dati personali dei dipendenti sono trattati attraverso il sistema di localizzazione per esigenze organizzative e produttive e che pertanto eventuali operazioni di trattamento effettuate allo scopo ulteriore di contestare illeciti disciplinari ai dipendenti non siano conformi al principio di finalità del trattamento (cfr. art. 11, comma 1, lett. b) del Codice); ritenuto che tali ulteriori trattamenti non siano altresì conformi alla disciplina posta in materia di controllo a distanza dei dipendenti, laddove vieta di installare dispositivi allo scopo di effettuare un controllo sull'attività lavorativa (cfr. art. 4, l. 20.5.1970, n. 300);
CONSIDERATO che in base al principio di proporzionalità, pertinenza e non eccedenza del trattamento rispetto alle finalità perseguite (art. 11, comma 1, lett. d) ed e) del Codice) il titolare è tenuto ad individuare i tempi di conservazione delle diverse tipologie di dati personali trattati;
RITENUTO di dover prescrivere alla società di predisporre un'informativa da rendere non solo ai dipendenti bensì anche agli utenti del servizio e ai cittadini che potrebbero essere interessati dai trattamenti in esame in considerazione del prospettato utilizzo dei dati raccolti con il sistema di localizzazione (anche) in vista della precostituzione di elementi di prova in caso di sinistri, dunque per finalità di tutela dei diritti (cfr. artt. 11, comma 1, lett. a) e 24, comma 1, lett. f) del Codice); a tale scopo si ritiene che possa essere utilizzato un modello semplificato di informativa collocato sui veicoli forniti di dispositivo di localizzazione (v. provv.ti n. 370 del 4 ottobre 2011 [punto 4] e n. 368 del 29.11.2012, doc. web n. 2257616);
RITENUTO che nel rispetto del principio di necessità (art. 3 del Codice) la società dovrà, in caso di comunicazione a terzi (segnatamente: centrale operativa regionale e consorzi delle aziende di trasporto in base alla convenzione in atti stipulata tra la regione Calabria e l'università della Calabria nell'ambito del piano sull'infomobilità) dei dati di localizzazione – per finalità di controllo sullo svolgimento del servizio di trasporto pubblico locale nonché di fornitura di servizi di infomobilità ai cittadini ed utenti –, provvedere a far sì che gli autisti dei veicoli geolocalizzati non siano identificabili;

RITENUTO pertanto che il descritto trattamento risulta effettuato dalla società, nei termini di cui in motivazione, in violazione della disciplina di protezione dei dati personali nonché della rilevante disciplina di settore (artt. 11, comma 1, lett. a), b), e) e 114 del Codice in relazione all'art. 4, comma 2, l. n. 300/1970);
CONSIDERATO che, ai sensi degli artt. 143, comma 1, lett. b) e 154, comma 1, lett. c), del Codice il Garante può prescrivere anche d'ufficio le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti;
RITENUTO pertanto di dover prescrivere alla società, quali misure necessarie al fine di rendere i trattamenti effettuati conformi alla disciplina in materia di protezione dei dati personali, di:
- attivare le procedure previste dal richiamato art. 4, comma 2, l. n. 300/1970, fatti salvi nel frattempo i diritti dei lavoratori, in relazione al trattamento dei dati di localizzazione;
- non utilizzare i dati trattati attraverso i sistemi di videosorveglianza e di geolocalizzazione per finalità di contestazione disciplinare in violazione della vigente disciplina in materia di controlli a distanza dei lavoratori;
- individuare congrui tempi di conservazione dei dati di localizzazione, in applicazione del principio di proporzionalità, in relazione alle finalità perseguite;
- predisporre un'informativa semplificata da apporre in modo visibile sui veicoli geolocalizzati;

- con particolare riferimento all'attività di localizzazione, in caso di comunicazione a terzi, procedere preliminarmente all'anonimizzazione dei dati personali trattati;
RILEVATO che, in caso di inosservanza del presente provvedimento, si renderà applicabile la sanzione di cui all'art. 162, comma 2-ter del Codice;
RISERVATA la possibilità di verificare, con autonomo procedimento, la sussistenza di illeciti amministrativi con particolare riferimento all'omessa informativa e notificazione al Garante (ai sensi dell'art. 37, comma 1, lett. a) del Codice) del trattamento dei dati di localizzazione anteriormente all'8.10.2013;
VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;
RELATORE il dott. Antonello Soro;
TUTTO CIÒ PREMESSO, IL GARANTE
nei confronti di A.M.A.CO. s.p.a. di Cosenza:
1. ritenuto illecito, nei termini di cui in motivazione, il trattamento effettuato a mezzo del sistema di localizzazione dei veicoli aziendali prescrive, ai sensi dell'art. 154, comma 1, lett. c) e 143, comma 1, lett. b) e 144 del Codice, di:
a. attivare senza ritardo le procedure previste dal richiamato art. 4, comma 2, l. n. 300/1970, fatti salvi nel frattempo i diritti dei lavoratori;
b. individuare congrui tempi di conservazione dei dati in relazione alle finalità perseguite;
c. predisporre un'informativa semplificata da apporre in modo visibile sui veicoli geolocalizzati;
d. procedere preliminarmente all'anonimizzazione dei dati personali trattati in caso di comunicazione a terzi;
e. non utilizzare i dati trattati per finalità di contestazione disciplinare in violazione del principio di finalità e della vigente disciplina in materia di controlli a distanza dei lavoratori;
2. con riferimento ai dati personali trattati attraverso il sistema di videosorveglianza prescrive quale misura necessaria, ai sensi dell'art. 154, comma 1, lett. c) e 143, comma 1, lett. b) e 144 del Codice, di non utilizzare i dati trattati per finalità di contestazione disciplinare in violazione del principio di finalità e in violazione della vigente disciplina in materia di controlli a distanza dei lavoratori;
3. ai sensi dell'art. 157 del Codice, invita la società a dare comunicazione al Garante delle misure adottate entro 40 giorni dalla data di ricezione del presente provvedimento.
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, 2 ottobre 2014

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia