Ufficio studi ed analisi di settore

FederSicurezza

Privacy e vigilanza privata

Collana quaderni
Giugno 2009
numero 2

Ufficio studi ed analisi di settore

FederSicurezza

Privacy e vigilanza privata

P.zza G.G.Belli 2, 00153 Roma - tel. +39.06.5866260 - fax. +39.06.5812750 - federsicurezza@confcommercio.it - www.federsicurezza.it

Presentazione del Presidente di Federsicurezza, Avv. Luigi Gabriele

Siamo al secondo quaderno, nella speranza che la pubblicazione del primo abbia riscontrato consenso e sia stato parimenti utile ai destinatari.

Se volessimo basarci sui riscontri epistolari, potremmo dichiararci soddisfatti.

Diciamo che,invece, preferiamo ritenerci motivati ad andare avanti, sperando di centrare ancora l'obiettivo.

Parliamo questa volta di un argomento delicato e, quanto ai risvolti applicativi, non proprio pacifico.

Ci siamo spinti a scriverne anche in considerazione del brillante esito avuto dal Corso di formazione che la nostra sempre più attiva Sicurservizi ha svolto tempo addietro, con notevole affluenza di manager e quadri d'Istituto, affluenza alla quale hanno fatto seguito istanze di ripetizione del Corso che periamo di poter soddisfare al più presto sperimentando questa volta la delocalizzazione dell'attività formativa resa all'utenza di comparto.

L'argomento, come dicevamo in apertura, ha valenza particolare in generale e ancora maggiore nel nostro segmento di attività, considerata la mole di dati sensibili che viene affidata ai nostri operatori.

Correttezza e professionalità in un campo così delicato contribuiranno a costituire valore aggiunto a quella piramide di qualità che con pazienza – non proprio certosina a volte – cerchiamo quotidianamente di contribuire a costruire perché, nel grande deserto dell'incertezza e del dubbio di una travagliata palingenesi normativa e regolamentare, dia con la propria ombra respiro agli addetti ai lavori che ormai sono a corto anche di…sudore, vista e misurata la quantità di ..lacrime e sangue versate nell'ultimo periodo sull'altare del mercato, in un contesto.. onirico così sintetizzabile: addormentarsi in un sogno per svegliarsi in un incubo!

Tornando a praticare un profilo credibile, noi operiamo con l'obiettivo della edificazione di un contesto di utilità buona per tutti coloro che riterranno di avvalersene, a prescindere dalle tante, forse troppe, appartenenze.

Il nostro voler fare sistema parte dal presupposto di voler essere sistema.
Il nostro fornire contributi non vuole essere fare vetrina, anche se le valenze dei professionisti e le professionalità alle quali ci rivolgiamo, come abbiamo fatto anche in questo caso, potrebbero consentirci di farlo.

Speriamo di essere compresi, di non essere giudicati invasivi, di essere aiutati a migliorare la qualità del nostro impegno.

Speriamo, dandovi la nostra lettura della privacy, di non arrivare a ..violare la Vostra.

Grazie ed arrivederci alla prossima puntata

Luigi Gabriele

VIGILANZA PRIVATA E RISPETTO DELLA PRIVACY: non una contraddizione ma materie complementari

Il diritto alla privacy è stato ed è tuttora oggetto di numerose discussioni, analisi accademiche e legislazioni nazionali ed internazionali, ma è ancor oggi impossibile trovarne una definizione chiara e condivisa, sebbene tale diritto sia universalmente considerato come uno dei diritti fondamentali di ogni cittadino. Data la mancanza di tale definizione, possiamo attenerci alla piuttosto semplice ma altrettanto limpida nozione del "diritto di essere lasciato solo".

Molti testi giuridici nazionali e internazionali affrontano il problema nell'ottica della protezione dei dati personali,considerando questi dati come informazioni che consentono, in maniera diretta o indiretta (in combinazione con altre informazioni) l'identificazione di una persona. In altre parole, la tutela della privacy comprende il diritto alla protezione da un uso illegale delle informazioni personali che possano ricondurre all'identità dell'individuo.

Purtroppo non è facilmente definibile il bilanciamento fra l'uso legale ed illegale dei dati personali e la protezione di questi mette in opera un procedimento altrettanto difficile da gestire.

Nel fare riferimento a due fondamentali testi giuridici europei, diventa più chiaro cosa si intende per "tutela dei dati personali". La DIRETTIVA 95/46/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, delinea all'articolo 7 i casi in cui gli Stati membri dell'Unione europea possano acconsentire al trattamento dei dati personali con un elenco esaustivo di casi. Gli Stati membri devono disporre a che i dati personali possano essere trattati solo se:

a) la persona interessata ha manifestato il suo consenso in maniera inequivocabile, oppure
b) è necessario all'esecuzione del contratto concluso con la persona interessata o all'esecuzione di misure pre-contrattuali prese su richiesta di tale persona, oppure
c) è necessario per adempire un obbligo legale al quale è soggetto il responsabile del trattamento, oppure
d) è necessario per la salvaguardia dell'interesse vitale della persona interessata, oppure
e) è necessario per l'esecuzione di un compito di interesse pubblico o commesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati, oppure
f) è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell'articolo 1 (1).

Inoltre, all'articolo 8.1 Gli Stati membri vietano il trattamento dei dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento dei dati relativi salute ed alla vita sessuale. Una serie di eccezioni vengono poi elencate.

Il Consiglio d'Europa ha adottato nel 1981 la Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale. Lo scopo della Convenzione è quello di garantire, sul territorio di ogni Parte, ad ogni persona fisica, qualunque siano la sua cittadinanza o residenza, il rispetto dei diritti e delle libertà fondamentali, ed in particolare del diritto alla privacy, nei confronti dell'elaborazione automatizzata dei dati di carattere personale che la riguardano ("protezione dei dati"). A tale riguardo la Convenzione stabilisce che i dati di carattere personale indicanti l'origine razziale, le opinioni politiche, le convinzioni religiose o altri credo, nonché i dati a carattere personale relativi allo stato di salute ed alla vita sessuale, non possono essere elaborati automaticamente a meno che il diritto interno non preveda garanzia adatte. Lo stesso dicasi dei dati di carattere personale relativi alle condanne penali.

Essenziale e importante in entrambi i testi giuridici europei è che la protezione dei dati personali si applica sia nel settore pubblico che nel settore privato e che impongono agli Stati membri di astenersi dal trattamento automatizzato di questi dati, salvo che il diritto interno preveda adeguate misure di salvaguardia.

Torniamo ora alla vigilanza privata. Trend generale ed irreversibile, nella maggior parte dei paesi europei, è che la sicurezza privata venga chiamata a svolgere un ruolo sempre più importante nel pubblico interesse; sta diventando un mezzo ed uno strumento della pubblica sicurezza. Un ulteriore tendenza è quella di vedere i servizi di sicurezza privata basarsi sempre più su tecniche e strumenti tecnologici; sebbene la componente umana nei servizi di sicurezza privata rimanga essenziale, gli agenti esercitano sempre più le proprie funzioni con l'ausilio della tecnologia. Il progresso in questo settore porta ad una maggiore sofisticatezza ed aumenta le potenzialità di questi strumenti. Proprio questi, però, potrebbero aprire la strada a più facili e meno controllati "abusi" nell'utilizzo dei dati personali. Un equilibrio deve essere quindi stabilito ed è responsabilità e dovere di ogni paese di occuparsene direttamente.

E' convinzione di CoESS che rientri fra le responsabilità delle autorità nazionali, e solo delle autorità nazionali, stabilire il giusto quadro giuridico regolante la sicurezza privata; questo deve naturalmente proteggere i cittadini contro i possibili abusi dal settore e di garantire, in via generale, che nessun elemento criminale possa infiltrarsi nel mercato. Ma essa deve anche consentire al settore di massimizzare la propria competenza, svolgere i propri compiti e fornire i propri servizi in modo competitivo e di rispondere alla crescente domanda di partecipazione alla soddisfazione del pubblico interesse cui è sovente chiamata. E' quindi ulteriore convinzione di CoESS che, qualora entri in gioco la protezione dei dati personali, le autorità nazionali abbiano la responsabilità di tradurre le misure di salvaguardia imposte a livello internazionale in modo tale che, da un lato, lo sfruttamento abusivo di questi dati da parte di soggetti operanti nel settore della sicurezza privata sia impossibile, ma , d'altro canto, che non siano di ostacolo al pieno svolgimento delle loro funzioni, in particolare quelle richieste o sovraintese dal committente pubblico.

CoESS è fermamente convinta che gli istituti di sicurezza privata non dovranno mai diventare un sostituto della pubblica sicurezza. Non è il nostro ruolo, né la nostra ambizione, né la nostra vocazione. La nostre compagnie sono in grado di supportare, aiutare e collaborare con le forze di pubblica sicurezza, ma in un quadro ben definito, con regole chiare, divisione delle responsabilità e ed un rigoroso ed efficace sistema di controllo. Gli stessi principi e lo stesso approccio devono essere applicati alla protezione dei dati personali quando raccolti, utilizzati, trattati o conservati da istituti di sicurezza privata.

CoESS pertanto condivide pienamente i principi generali elencati nei due testi giuridici europei di cui sopra. Per citare la Convenzione 108 del Consiglio d'Europa, "I dati a carattere personale oggetto di un'elaborazione automatizzata sono:

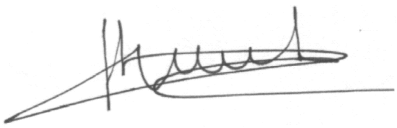
a) ottenuti e elaborati in modo lecito e corretto;
b) registrati per scopi determinati e legittimi ed impiegati in una maniera non incompatibile con detti fini;
c) adeguati, pertinenti e non eccessivi riguardo ai fini per i quali vengono registrati;
d) esatti e, se necessario, aggiornati;
e) conservati in una forma che consenta l'identificazione delle persone interessate per una durata non superiore a quella necessaria ai fini per i quali sono registrati."

Un altro elemento fondamentale è il diritto di accesso ai dati. Questi criteri devono essere completamente applicati anche quanto i dati sono trattati da istituti di sicurezza privata.

Tuttavia, CoESS è anche del parere che vi sia un margine sufficientemente ampio tra ciò che è consentito e non consentito riguardo alla protezione dei dati personali. In altre parole, è essenziale, per l'ulteriore sviluppo dei servizi e dei compiti del nostro settore, che il legislatore nazionale trovi il giusto equilibrio tra la

tutela della privacy di ogni cittadino e l'ulteriore progresso nell'utilizzo di tecnologie. Un indicatore importante per stabilire questo equilibrio è la percezione collettiva e la maggiore accettazione da parte del pubblico di tecnologie quali telecamere ed altri sistemi di video-sorveglianza, la raccolta e memorizzazione di dati automatizzata, sistemi di ingresso e di uscita sorvegliati elettronicamente, ecc. Un altro elemento importante è la certezza che il settore della sicurezza privata in molti paesi si sia sviluppato e sia maturato attraverso una grande responsabilità e professionalità: il personale è addestrato e controllato intensamente, il controllo interno e l'auditing sono standard e prassi comune; la qualità, in generale, è un concetto integrato di business e la corporate governance una delle priorità. Deve quindi essere chiaro che nella delicata materia della tutela della privacy, attraverso il trattamento dei dati personali, gli istituti di sicurezza privata possono e devono assumersi le loro responsabilità e, quindi, ancora una volta, essere un elemento essenziale di cooperazione per l' autorità pubblica.

Hilde de Clerck
General Secretary of CoESS[1]



[1] Confederation of European Security Services

PRIVACY E VIGILANZA PRIVATA

Premessa

Per delle imprese che vendono "sicurezza", quali sono gli istituti di vigilanza privata, non può non interessare la protezione e la sicurezza dei dati e delle informazioni, e ciò non solo e non tanto perché c'è una legge italiana di derivazione europea che da quasi tredici anni ormai si occupa di questo tema, dettandone una particolare disciplina, ma perché saper proteggere, oltre ai beni ed ai valori affidati, anche le informazioni che i clienti comunicano e/o trasmettono all'azienda, può rappresentare un vantaggio competitivo non indifferente, che potrebbe essere determinante nell'aggiudicarsi un servizio e nel manlevare l'azienda da eventuali richieste di risarcimento danni o dal rischio di incorrere in responsabilità penali od amministrative. A ciò si aggiunga che lo svolgimento in outsourcing di certi servizi di vigilanza, quale la videosorveglianza, se effettuato, ad esempio, in violazione della legge penale, può comportare il rischio di essere chiamati a rispondere, con il cliente, di concorso nel reato di interferenze illecite nella vita privata previsto dall'art. 615 bis cod. pen., piuttosto che il configurarsi di una corresponsabilità di natura civile, per aver causato un danno a terzi, o di natura amministrativa, per non aver compiuto un adempimento obbligatorio.
Se poi si considera che l'esperienza insegna che gli incidenti sulla sicurezza (quali la fuga di dati o la perdita di riservatezza) sono provocati più spesso da errori umani che dal guasto di un meccanismo elettronico o di un sistema, ecco allora diventare di fondamentale importanza la formazione, in quanto l'essenza della sicurezza non risiede nelle soluzioni tecniche, ma nella coscienza, nella cultura, nella consapevolezza delle persone. Formazione significa anzitutto conoscenza della normativa di riferimento, condizione imprescindibile per l'acquisizione di un comportamento consapevole dal punto di vista della sicurezza dei dati, e ciò ad iniziare dal legale rappresentante della società, che riveste un ruolo centrale nella strategia di protezione aziendale.
Ne consegue che, anche per le imprese di vigilanza, è importante sapere cosa occorre fare per proteggere al meglio i dati e le informazioni, come farlo e quando farlo, dal momento che la legge sulla privacy prevede alcuni adempimenti periodici e richiede un costante aggiornamento delle misure di sicurezza adottate, senza tuttavia mai dimenticare che, al di là di ogni tecnicismo e formalismo, l'applicazione del buon senso resta sempre la più solida base della sicurezza.
Scopo di questo secondo numero dei *Quaderni* editi da FederSicurezza è di offrire una guida per le imprese operanti nel settore della vigilanza privata, di modo da far conoscere quali sono gli adempimenti generali che sono tenute ad adottare, oltre a quelli particolari previsti per la videosorveglianza e gli amministratori di sistema, fermo restando il carattere non esaustivo della presente trattazione, la quale non può tenere conto dei contesti operativi particolari di ogni azienda.

1. Adempimenti

Premesso che per "dato personale" è da intendersi "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale" (art. 4 comma 1 lett. b Codice Privacy), nelle loro quotidiane attività aziendali gli istituti di vigilanza trattano diversi dati personali (es.: dati anagrafici, partiva iva, codice fiscale, indirizzi email) in ragione dello svolgimento delle più comuni attività d'impresa (es. trattamento economico e giuridico del personale, gestione dei fornitori e dei clienti) e di attività specifiche proprie delle imprese di tale settore (es. videosorveglianza per conto terzi) o, ancora, effettuano trattamenti di dati con tecnologie che possono

presentare particolari rischi in relazione alla protezione dei dati (es. utilizzo del sistema satellitare GPS per la radiolocalizzazione degli automezzi aziendali destinati al trasporto valori).
Come già accennato, i dati personali sono oggetto di una particolare disciplina contenuta nel Codice Privacy (D.Lgs. 30 giugno 2003 n.196, di seguito anche "Cod. Priv.") e nel Disciplinare Tecnico Allegato B al Codice, in vigore dall'1 gennaio 2004, che ha abrogato la normativa precedente costituita dalla legge 675/96 e dal D.P.R. 318/99. Tale disciplina ha lo scopo di tutelare la circolazione dei dati sin dal momento della loro raccolta, prescrivendo in capo al Titolare del trattamento una serie di adempimenti che, sostanzialmente, possono suddividersi in due macrocategorie: (i) le misure organizzative e (ii) le misure logiche.
Prima di procedere alla disamina delle suddette misure, è opportuno però chiarire da subito che 'Titolare del trattamento' per legge, è **la società** in persona del legale rappresentante pro tempore "cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza"(art. 4 comma 1 lett. f e art. 28 Cod. Priv.). Ne deriva che il Titolare del trattamento è un soggetto individuato di diritto, nel senso che non occorre una nomina od una procura specifica per essere Titolari, in quanto il legale rappresentante ha per legge tutti i poteri necessari per l'adempimento del Codice Privacy.

1.1 Misure organizzative

Qui di seguito sono illustrati i caratteri principali delle misure organizzative che devono essere adottate anche dagli istituti di vigilanza privata a garanzia del corretto trattamento dei dati, consistenti in una serie di documenti da predisporre, nonché nell'attività di formazione e vigilanza, entrambe da svolgersi periodicamente.

- **Informativa agli Interessati - e richiesta dell'eventuale consenso al trattamento e/o alla comunicazione dei dati**

Ogniqualvolta i suoi dati sono trattati da terzi, l'Interessato (ossia "*la persona fisica, giuridica, l'ente o l'associazione cui si riferiscono i dati personali*" ex art. 4 comma 1 lett. *i* Cod. Priv.) ha diritto di ricevere dal Titolare determinate informazioni, che devono essere espressamente indicate nell'Informativa, la quale costituisce il principale adempimento a tutela dell'Interessato in attuazione dei principi di lealtà e trasparenza, facendogli conoscere, tra l'altro, l'origine e gli scopi per i quali i suoi dati sono trattati e comunicati, permettendogli di esprimere un consenso valido al trattamento dei dati (nei casi in cui è ancora richiesto) e mettendolo in condizione di esercitare nei confronti del Titolare alcuni diritti riconosciuti dal Codice Privacy.
L'Informativa deve essere rilasciata una sola volta al momento della raccolta dei dati, se i dati sono raccolti presso l'Interessato, oppure all'atto della registrazione dei dati o non oltre la prima comunicazione, se i dati sono raccolti presso terzi. Anche quando non è richiesto il consenso per il trattamento dei dati personali, l'Informativa deve essere sempre data, oralmente o per iscritto, ma è consigliabile la forma scritta per l'assolvimento dell'onere della prova incombente sul Titolare.
Quanto al contenuto, esso è stabilito dall'art. 13 del Cod. Priv., anche se vi è la possibilità di rilasciare un'Informativa orale e breve, che rinvii ad un testo più articolato agevolmente disponibile, ad esempio, tramite reti Intranet o siti Internet, affissioni in bacheche o locali, avvisi e cartelli agli sportelli o, ancora, messaggi preregistrati.
Alla luce di quanto sopra deriva che gli istituti di vigilanza privata devono dare l'Informativa a tutti gli Interessati di cui trattano i dati personali, quali, ad esempio, i dipendenti ed i lavoratori ad essi assimilati (es. collaboratori a progetto), i candidati, gli amministratori, i sindaci, i soci, le controllate e controllanti, i fornitori (anche potenziali), i consulenti, i clienti (anche potenziali), gli agenti, i visitatori e gli utenti-navigatori del sito web aziendale.

L'omessa o inidonea Informativa rappresenta la violazione amministrativa più sanzionata dal Garante della privacy, con una sanzione oggi compresa tra un minimo di € 6.000,00 ad un massimo di € 36.000 (art. 161 Cod. Priv. come modificato dalla Legge 27.02.09 n. 41), importi aumentabili fino al quadruplo, a discrezione del Garante, in ragione delle condizioni economiche dell'azienda (art. 164 bis comma 4 Cod. Priv.).
Salvo i casi di esenzione, il consenso per il trattamento e/o la comunicazione dei dati deve essere chiesto e ottenuto preventivamente in modo libero e specifico (art. 23 Cod. Priv.). Al riguardo, il Codice Privacy ha introdotto un'importante semplificazione, poiché ha disposto che per le aziende private il consenso non è necessario quando i dati trattati: a) sono di *fonte pubblica* (ossia provengono da pubblici registri ed elenchi pubblici conoscibili da chiunque, come I registri delle imprese presso la Camera di Commercio); b) sono *necessari per eseguire un contratto od obblighi precontrattuali o per adempiere a ordinarie finalità amministrative e contabili*; c) *riguardano attività economiche dell'Interessato* (es. Informazioni sul fatturato, sulla quantità di merci vendute, su insolvenze o ritardi di pagamento); d) sono *necessari per adempiere ad un obbligo di legge* (es. dati sensibili nei rapporti di lavoro e i dati anagrafici e fiscali dei dipendenti) (art. 24 Cod. Priv.).
La mancata richiesta del consenso, quando è obbligatorio, rende il trattamento o la comunicazione dei dati illegittimi ed i dati inutilizzabili.

- ## Nomina a Incaricato del trattamento

'Incaricato del trattamento' è la "*persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile*" (art. 4 comma 1 lett. *h* ed art. 30 Cod. Priv.): Incaricato è il dipendente o collaboratore della società che materialmente esegue le operazioni di trattamento dei dati personali attenendosi alle istruzioni impartite dal Titolare o dal Responsabile.
La designazione a Incaricato deve essere fatta con apposita lettera che, oltre alle istruzioni impartite, riporta il profilo di autorizzazione del lavoratore (ovvero indica a quali archivi o banche dati può avere accesso e con quali eventuali limitazioni). Almeno una volta all'anno detto profilo deve essere verificato e la nomina a Incaricato aggiornata di conseguenza, se del caso.
La nomina a Incaricato *non comporta l'assegnazione di mansioni o di incarichi nuovi*, in quanto trattasi del mero riconoscimento delle attività svolte dal dipendente/collaboratore all'interno della società.
Ciò premesso, le imprese di vigilanza privata devono nominare Incaricati tutti i lavoratori che compiono operazioni di trattamento di dati personali (es. raccolta, registrazione, consultazione, elaborazione, modifica, comunicazione, etc.) correlate alle mansioni e agli incarichi ricoperti; dovranno essere pertanto nominati Incaricati le impiegate, gli agenti, gli esattori, gli operatori della centrale operativa, le guardie particolari giurate, nonché il Rappresentante dei Lavoratori della Sicurezza (o "RLS"), che deve essere autorizzato a trattare i dati, anche sensibili, contenuti nel '*Documento di Valutazione dei Rischi*' o nel '*Registro degli Infortuni sul Lavoro*', oppure nelle copie di quelle parti di tali documenti di volta in volta richieste al datore di lavoro.

- ## Nomina a Responsabile del trattamento

Secondo la definizione di legge (art. 4 comma 1 lett. g e art. 29 Cod. Priv.), Responsabile del trattamento è "chi (persona fisica/giuridica) effettua trattamenti di dati personali operando sotto il diretto controllo del Titolare".
Per essere 'Responsabili del trattamento' (interni o esterni all'azienda) occorre essere stati nominati tali dal Titolare con apposito atto contenente le Istruzioni ed i compiti da quest'ultimo impartiti, atto da sottoscrivere da entrambe le parti.
Nominare uno o più Responsabili del trattamento è una facoltà riconosciuta al Titolare, ma consigliabile in realtà aziendali articolate ove il legale rappresentante non può presiedere a tutti i trattamenti di dati

effettuati in azienda. Nella prassi, alcune aziende nominano Responsabili interni i direttori di funzione/di filiale/di stabilimento o il responsabile di area, e Responsabili esterni la società o lo studio di consulenza che elabora le paghe e gli stipendi, o, ancora, la capogruppo che in outsourcing svolge per le controllate determinati servizi di staff.

- **Disciplinare o Policy per l'utilizzo delle risorse informatiche aziendali da allegare alla nomina degli Incaricati del trattamento.**

È un documento obbligatorio previsto dal Codice Privacy e richiesto dall'Autorità Garante con il Provvedimento dell'1 marzo 2007 intitolato "*Linee Guida del Garante per posta elettronica ed Internet*".
Scopo è definire i diritti e gli obblighi dei lavoratori (e del datore di lavoro) sul corretto utilizzo delle risorse informatiche aziendali, mediante la predisposizione di regole aziendali di comportamento atte ad evitare comportamenti inconsapevoli e/o scorretti da parte dei lavoratori in tema di sicurezza e protezione dei dati. Quanto al contenuto, la policy deve riportare le istruzioni concrete del datore di lavoro sull'applicazione delle misure di sicurezza adottate dall'azienda, indicare le regole per il corretto uso della posta elettronica aziendale e della navigazione in Internet, richiamando le responsabilità, i controlli e le sanzioni cui incorrerebbe il lavoratore in caso di mancato rispetto delle regole ivi contenute.

- **Formazione**

La formazione dei lavoratori, comprese le figure apicali dell'azienda, oltre a rispondere ad un obbligo di legge (regola 19.6 dell'Allegato B), ha lo scopo di rendere i lavoratori consapevoli dei rischi che incombono sui dati, delle misure disponibili in azienda per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali e delle responsabilità che ne possono derivare. Essa deve essere effettuata almeno all'ingresso in azienda e, successivamente, in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

- **Vigilanza Periodica (art. 29 comma 5 Cod. Priv.)**

È previsto che il Titolare verifichi, almeno una volta l'anno, l'osservanza delle disposizioni contenute nel Codice Privacy e delle istruzioni impartite in azienda in materia di tutela e sicurezza dei dati, documentando per iscritto tale attività in apposito report.

- **Notificazione telematica al Garante per il trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica**

Come anticipato nella Premessa, alcuni istituti di vigilanza privata utilizzano il sistema satellitare GPS per la localizzazione degli automezzi aziendali destinati al trasporto valori, che comporta la possibilità di localizzare la posizione geografica del veicolo di modo da facilitare un intervento tempestivo in aiuto del conducente in caso di necessità (es. assalto al furgone). Ebbene, l'uso di tale apparecchiatura elettronica comporta un trattamento di dati personali compreso tra quelli che devono essere ***preventivamente*** notificati al Garante (art. 37 punto *a* Cod. Priv.).

Il termine iniziale per effettuare la notifica era stato fissato al 30 aprile 2004, per quelle aziende che a quella data già utilizzavano il GPS, mentre se il GPS è stato utilizzato da una data successiva o, meglio, non è ancora stato utilizzato, la notifica deve essere effettuata prima dell'utilizzo del GPS. Nel caso in cui non sia stato ancora fatta la notifica, si consiglia di effettuarla sia pure tardivamente così, in caso di eventuale accertamento, si pagherebbe una sanzione sicuramente inferiore.
La notificazione può essere eseguita esclusivamente utilizzando l'interfaccia disponibile sul sito web del Garante, seguendo le istruzioni ivi indicate (art. 38 Cod. Priv.).
Numerosi sono ancora i casi in cui il Garante ha inflitto alle aziende la sanzione amministrativa del pagamento di un importo compreso tra € 20.000 e € 120.000 per omessa o incompleta notificazione (ex art. 163 Cod. Priv. come modificato dalla L. 41/2009 cit.).
Inoltre, affinché l'utilizzo del GPS sia legittimo, occorre, oltre alla notifica, anche l'accordo sindacale o, in mancanza, l'autorizzazione della Direzione Provinciale del Lavoro, in quanto il GPS potrebbe consentire un controllo indiretto dell'attività lavorativa tramite apparecchiature elettroniche, vietato dall'art. 4 dello Statuto dei lavoratori, la cui vigenza è confermata dall'art. 114 del Codice Privacy.

1.2 Misure logiche

Come ogni impresa, anche gli istituti di vigilanza privata sono obbligati ad adottare tutte le misure di sicurezza per prevenire i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Le misure di sicurezza previste dalla vigente normativa comprendono: le *a) misure minime*, che configurano il livello minimo di protezione richiesto in relazione ai rischi sopra individuati, la cui fonte è negli artt. 33-36 Cod. Priv. e nell'Allegato B; le *b) misure idonee e preventive* (art. 31 Cod. Priv.), che si aggiungono alle prime, sono considerate idonee ad evitare il danno e sono desumibili dallo stato dell'arte in relazione alla natura dei dati trattati ed alle caratteristiche del trattamento. La mancata adozione delle misure idonee può dare luogo a responsabilità civile con la conseguente sanzione del risarcimento del danno ex art. 15 Cod. Priv.: *"Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 cod. civ."*.
Di seguito si riporta un elenco di quelle che sono le misure minime di sicurezza per i trattamenti di dati effettuati con strumenti elettronici, indicando, per ciascuna, il riferimento di legge cui si rinvia per conoscerne le modalità tecniche di attuazione, argomento che esula dalla presente trattazione.

Misure minime di sicurezza per i trattamenti dati con strumenti elettronici:

1) sistema di autenticazione informatica basata sull'uso di credenziali di autenticazione (art. 34 lett. *a* e *b* Cod. Priv.; per le modalità applicative si rinvia alle regole di cui ai punti 1, 2, 3, 5, 6, 7, 8, 10 e 11 dell'Allegato B);
2) procedura per la gestione delle credenziali di autenticazione (regole di cui ai punti da 6 a 11 dell'Allegato B);
3) utilizzo di un sistema di autorizzazione (art. 34 lett. *c* e *d* Cod. Priv.; regole da 12 a 14 dell'Allegato B);
4) aggiornamento periodico individuazione ambito trattamento consentito ai singoli incaricati o addetti alla gestione o alla manutenzione degli strumenti elettronici (regola 15 dell'Allegato B);
5) altre misure di sicurezza (es. antivirus, firewall, aggiornamento del sistema operativo: regole da 15 a 18 dell'Allegato B);
6) salvataggio dei dati ogni sette giorni (regola 18 Allegato B);
7) procedura per la custodia copie di sicurezza (regola 19.5 Allegato B);
8) aggiornamento del Documento Programmatico sulla Sicurezza entro il 31 marzo di ogni anno (regola 19 Allegato B).

La mancata adozione delle misure minime di sicurezza rappresenta a tutt'oggi la violazione penale più contestata dal Garante nel corso delle ispezioni effettuate, punita con l'arresto sino a due anni con possibilità dell'oblazione del reato (contravvenzione), consistente nel pagamento volontario di una determinata somma; il pagamento estingue il reato (art. 169 comma 1 Cod. Priv.).

2. Videosorveglianza

La videosorveglianza è sempre più diffusa nel nostro Paese, ovunque infatti sono presenti telecamere: in luoghi e su mezzi pubblici di trasporto, negli esercizi commerciali, discoteche, piscine, scuole, ospedali, luoghi di cura e di culto, banche, centri sportivi e aziende. Occorre però sapere che l'uso di telecamere può ledere diritti altrui, quali il diritto alla riservatezza, alla dignità ed alla libertà degli individui e dei lavoratori (nel caso la videosorveglianza sia effettuata nell'ambito di un contesto lavorativo), diritti tutti tutelati, oltre che dalla Costituzione, da leggi dello Stato sia civili che penali, per cui occorre prestare molta attenzione al riguardo.
La normativa vigente sulla videosorveglianza è costituita, oltre che dal Codice Privacy e dall'Allegato B, dal Provvedimento Generale sulla Videosorveglianza del 29 aprile 2004, emanato dall'Autorità Garante per la tutela dei dati personali allo scopo di salvaguardare la sicurezza dei cittadini ed il loro diritto alla riservatezza, con il limite, tuttavia, che esso contiene delle prescrizioni lontane dalla realtà pratica delle aziende e troppo generiche, ma che, in ogni caso, devono essere obbligatoriamente osservate da parte di tutti i soggetti, pubblici e privati, chiamati a gestire un sistema di videosorveglianza, anche per conto terzi, pena il rischio di incorrere in responsabilità giuridiche, di natura anche penale.
La videosorveglianza comporta un trattamento di dati personali, come tale rilevante per la normativa sopracitata, ogniqualvolta le telecamere effettuano delle riprese riferibili, anche indirettamente (es. numero di targa), ad una persona fisica, giuridica, ente o associazione. Ne consegue che si è fuori dal campo di applicazione della normativa in esame quando le riprese riguardano esclusivamente dati anonimi o consentono di rilevare immagini di così scarsa definizione da non consentire il riconoscimento degli individui (es. *web cam* sulle spiagge o in stazioni sciistiche per la ripresa di insieme dei luoghi), oppure, ancora, quando i dati sono trattati per scopi esclusivamente personali.
Nell'ambito della vigilanza privata la videosorveglianza può essere svolta sia nell'interesse e per conto dell'istituto di vigilanza, allo scopo di presidiarne gli accessi alla sede (c.d. 'videosorveglianza perimetrale esterna') o l'accesso a determinati locali interni in cui sono custoditi beni e valori rilevanti (es. sala conta, con telecamere sia ambientali che sulle postazioni di lavoro; caveau e autorimessa, con telecamere solo ambientali, e nei locali ad essi antistanti o adiacenti), sia per conto di terzi, come servizio ai clienti. Nell'un caso o nell'altro gli istituti sono tenuti a rispettare, anzitutto, i principi fondamentali di riferimento qui di seguito indicati:

A) Liceità: i dati (ossia le immagini) rilevati con le telecamere devono essere sempre trattati in modo lecito e secondo correttezza, nel rispetto non solo della normativa sulla videosorveglianza, ma di ogni altra legge (es. statuto dei lavoratori, codice penale, il cui art. 615 bis contempla il reato di '*interferenze illecite nella vita privata*', che si riscontra quando ci si procura indebitamente immagini o notizie attinenti alla vita privata svolgentesi in luoghi di privata dimora). Ciò significa che gli enti pubblici possono effettuare la videosorveglianza solo per perseguire le funzioni istituzionali, mentre le imprese private possono effettuarla per l'adempimento ad un obbligo di legge, o in attuazione del c.d. 'bilanciamento degli interessi' di cui al Provvedimento Generale del Garante del 29.04.04 allo scopo di tutelare persone e beni da aggressioni, furti, vandalismo, o, ancora, in presenza di un consenso libero ed espresso da parte dei soggetti cui le immagini si riferiscono. Nella prassi, il Garante ha riconosciuto legittima la videosorveglianza effettuata da imprese private per finalità di protezione delle persone, della proprietà e del patrimonio aziendale, nonché per quelle imprese che svolgono attività che comportano la presenza di denaro o di beni di valore.

B) Finalità: le immagini devono essere raccolte e trattate per scopi determinati, espliciti e legittimi, enunciati nell'Informativa. È stabilito che ciascuno può perseguire solo scopi di sua pertinenza, per cui il Garante più volte ha affermato che né gli enti pubblici né le imprese private possono effettuare la videosorveglianza per scopi di sicurezza pubblica o di prevenzione ed accertamento dei reati, in quanto tali finalità competono esclusivamente all'autorità giudiziaria ed alle forze di polizia. Sempre con riferimento al principio di finalità, è stata riconosciuta la legittimità della videosorveglianza effettuata per scopi pubblicitari con telecamere, ad esempio, collocate presso località turistiche o stazioni ferroviarie, purché le riprese siano panoramiche e le immagini di scarsa definizione, senza la possibilità di zoom né di modifica dell'inquadratura.

C) Necessità: devono essere esclusi usi superflui ed evitate eccessive ridondanze; inoltre, è prescritto di ridurre al minimo l'uso di immagini di dettaglio riferibili a soggetti determinati e, nell'eventualità, esse potrebbero essere utilizzate solo in caso di stretta necessità.

D) Proporzionalità: le immagini riprese con le telecamere non devono essere eccedenti rispetto alle finalità legittimamente perseguite dal Titolare del trattamento (dichiarate nell'Informativa) e possono essere conservate solo per il tempo necessario in relazione allo scopo per il quale esse sono raccolte e trattate. Il ricorso alla videosorveglianza è consentito solo quando altre misure di sicurezza sono da ritenersi insufficienti od inattuabili: è illecito utilizzare tecnologie (quali la videosorveglianza) sproporzionate allo scopo o riprendere aree non soggette a concreti pericoli e non ricomprese nelle finalità lecitamente perseguite dall'azienda.

Costituisce un corollario del principio di proporzionalità l'obbligo di limitare la raccolta di immagini dettagliate, l'angolo visuale di ripresa, l'utilizzo di zoom automatici, la registrazione delle immagini e la conseguente durata di conservazione, la creazione di database, l'indicizzazione delle immagini e l'interconnessione del sistema di videosorveglianza con sistemi gestiti da terzi.
Quanto alla durata della conservazione, il Provvedimento del 29.04.04 prescrive la regola generale secondo cui le immagini possono essere conservate poche ore o, al massimo 24 ore; la conservazione per un tempo ulteriore (es. 48 o 72 ore o una settimana) è prevista solo in caso di festività o di chiusura di uffici o esercizi, nonché per aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o della polizia giudiziaria.
Sul punto, è notizia del febbraio scorso che il Garante, nei confronti di un supermercato toscano che aveva posto delle telecamere "presso gli accessi alle aree di scarico merci" e "all'interno del box informazioni" che registravano su disco rigido le immagini rilevate sino a 72 ore, ha prescritto di commisurare il tempo di conservazione delle immagini alle effettive necessità della raccolta secondo i termini previsti nel citato provvedimento generale, disponendo altresì il blocco dell'ulteriore trattamento dei dati così effettuato (cfr. Newsletter del Garante del26.02.09).
Sempre in tema di durata di conservazione, si segnala che il decreto antistupri, di recente emanazione, autorizza i Comuni ad utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana, consentendo espressamente la conservazione dei dati, delle informazioni e delle immagini così raccolte fino a sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione.
Da quanto sopra deriva che le immagini eventualmente registrate devono poi essere cancellate automaticamente dal sistema e da ogni supporto rimovibile dopo un certo tempo, con modalità da renderle non più riutilizzabili. Tuttavia, ancora molti sistemi di videosorveglianza presenti sul mercato non consentono la cancellazione automatica delle immagini ad un tempo prefissato, ma solo la riscrittura a disco pieno (o porzione prefissata di disco); ebbene, tali software non soddisfano i requisiti sulla durata di conservazione imposti dal Garante, e, pertanto, comportano una violazione del principio di proporzionalità in esame, per cui sarebbe opportuno ricorrere quanto prima a software di nuova generazione che consentano la cancellazione automatica ed effettiva delle immagini alla scadenza prefissata.
Dopo aver esaminato quali sono i principi fondamentali da rispettare per qualsiasi sistema di videosorveglianza, si passano ora in breve rassegna gli adempimenti prescritti nel Provvedimento Generale

del Garante del 29.04.04, necessari affinché un sistema di videosorveglianza possa definirsi '*compliant*' ovvero 'conforme' a detta normativa:

1) Informativa: nelle aree esterne in prossimità dei luoghi ripresi dalle telecamere o nelle loro immediate vicinanze occorre collocare dei cartelli di Informativa, di modo che siano chiaramente visibili, utilizzando al riguardo il modello di Informativa semplificata dato dal Garante.
Oltre ai suddetti cartelli, è necessario che nell'Informativa rilasciata ai dipendenti questi ultimi siano informati che, qualora fossero addetti a determinati servizi (es. trasporto valori e contazione del denaro) od accedessero a particolari locali aziendali, per esigenze di sicurezza dei beni, dei valori e delle persone potrebbero essere attivati anche sistemi di videosorveglianza, dei quali troveranno opportuna indicazione nei luoghi in cui sono collocate le telecamere. Del pari, nel caso l'istituto di vigilanza effettui videosorveglianza per conto di clienti, anche questi devono ricevere una specifica Informativa sulla videosorveglianza, in cui siano avvisati che, tra le finalità correlate all'esecuzione del contratto, è compresa la raccolta e l'eventuale registrazione delle immagini rilevate, ad esempio, in caso di allarme, mediante telecamere installate presso il loro sito.
Nel contratto di videosorveglianza sarebbe opportuno specificare che resta a carico del cliente, Titolare del trattamento della videosorveglianza, l'obbligo di apposizione dei cartelli di Informativa, così come sarebbe auspicabile inserire una clausola contente la richiesta al cliente di garanzia circa la liceità del trattamento delle immagini riprese e l'esclusione di ogni violazione a norme di legge (in particolare, allo Statuto dei Lavoratori), nonché un'altra clausola di manleva a favore dell'istituto appaltatore del servizio.

2) Nomina degli Incaricati alla visualizzazione delle immagini: occorre predisporre la nomina degli Incaricati al trattamento legittimati alla visualizzazione in tempo reale delle immagini e/o di quelle registrate, cercando di limitare il numero dei soggetti autorizzati ad accedere alle registrazioni in caso di necessità.

3) Accordo sindacale: è necessario anche per il solo caso della videosorveglianza perimetrale esterna all'istituto di vigilanza, ex art. 114 del Cod. Priv.; in mancanza di tale accordo è necessaria l'autorizzazione della Direzione Provinciale del Lavoro. Il difetto dell'accordo o della citata autorizzazione configura un illecito penale punibile con le sanzioni previste dall'art. 38 L. 300/1970.

4) Documentazione delle scelte: è un documento, da conservare presso la sede, in cui vanno descritte le motivazioni delle scelte effettuate dalla società in merito ai trattamenti effettuati con impianti di videosorveglianza.

5) Verifica preliminare (c.d. *"Prior Checking"*): devono essere sottoposti all'esame preventivo del Garante solo i trattamenti connessi ad alcuni sistemi individuati nel Provvedimento Generale del 29.04.04, quali i sistemi che consentono un'indicizzazione o digitalizzazione delle immagini, o per i sistemi di videosorveglianza 'dinamico-preventiva' (rilievo di eventi improvvisi) o che prevedono la raccolta di immagini collegata e/o incrociata con altri dati (es. voce, biometrici). Al riguardo il Garante ha precisato che l'utilizzo di un impianto di videosorveglianza digitale non comporta di per sé rischi specifici e, come tale, non deve essere sottoposto a verifica preliminare dell'Autorità; viceversa, l'utilizzo di tecniche avanzate di indicizzazione e di ricerca sulla base, ad esempio, di caratteristiche morfologiche e comportamentali degli Interessati, rientra nel caso in esame della verifica preliminare.

6) Notificazione telematica e preventiva al Garante: è necessaria solo se la videosorveglianza riguarda la raccolta di dati biometrici o che indicano in maniera continuativa la posizione geografica di persone o cose identificabili mediante rete di comunicazione elettronica (art. 37 Cod. Priv. lett. a).

7) Misure di sicurezza: anche per i sistemi di videosorveglianza devono essere adottate sia le misure idonee e preventive, valutabili caso per caso, sia quelle minime, e precisamente, credenziali di autenticazione diverse per ogni singolo utente, la procedura per la gestione delle credenziali, il sistema di autorizzazione

con diversi livelli di accesso al sistema di videosorveglianza, l'antivirus (costantemente aggiornato), la doppia chiave fisica o logica per l'accesso regolamentato alle immagini registrate esclusivamente in caso di necessità, l'attestazione di conformità dell'installatore.

8) Nomina a Responsabile del trattamento del manutentore del sistema e/o del terzo outsourcer: come in precedenza affermato, in genere la nomina a Responsabile del trattamento è una facoltà, e non un obbligo dell'azienda; tuttavia, si segnala che tale nomina sembra auspicabile dal Garante alla luce del provvedimento emesso il 2.10.08 (pubblicato sulla newsletter dell'Autorità del 16.01.09), con cui ha prescritto ad un Titolare del trattamento di nominare Responsabile la società manutentrice del sistema di videosorveglianza, in quanto unica legittimata ad accedere alle immagini registrate. Per analogia, in applicazione di tale principio, si dovrebbe ritenere che anche gli istituti di vigilanza privata che gestiscono in outsourcing tutto o parte del sistema di videosorveglianza per conto di clienti, dovrebbero essere nominati da questi ultimi Responsabili del trattamento.

3. Misure per gli Amministratori di Sistema

L'ultimo provvedimento di rilievo emesso, in ordine cronologico, dal Garante si intitola "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" emesso il 27.11.08 (pubblicato sulla G.U. n. 300 del 24.12.08). Il documento contiene alcune prescrizioni di carattere sia tecnico che organizzativo, che le aziende sono tenute ad adottare entro il 30 giugno 2009, termine già prorogato e, probabilmente, suscettibile di un'ulteriore proroga da parte dell'Autorità.
Scopo è quello di rendere più trasparente l'attività compiuta dagli amministratori di sistema, di modo da agevolare il Titolare nell'esercizio del dovere di controllo ad esso spettante per legge.
Il provvedimento in esame presenta delle lacune interpretative e definizioni troppo generiche, che rendono poco comprensibile alle aziende che cosa precisamente sono tenute a fare in materia, e la questione non è di poco conto, dal momento che il mancato adempimento a quanto prescritto dal Garante espone al rischio del pagamento di una sanzione compresa tra € 30.000 ed € 180.000 (art. 162 comma 2 ter Cod. Priv.).
Anzitutto, la nozione di 'amministratore di sistema' adottata dal Garante è molto ampia, poiché vi è compreso l'amministratore di rete, di basi di dati, di apparati di sicurezza e di sistemi software complessi, senza tuttavia che sia in qualche modo specificato cosa debba intendersi con tale ultimo termine. Pare che dal Provvedimento in esame siano tuttavia esclusi i trattamenti effettuati in ambito privato (e pubblico) a fini amministrativo-contabili (cfr. le risposte del Garante del 21.05.09 ai quesiti più frequenti in tema di misure per gli amministratori di sistema consultabili sulla home page del sito dell'Autorità www.garanteprivacy.it).
Quanto alle misure da adottare, è richiesta la designazione scritta ed individuale di amministratore di sistema, previa valutazione delle caratteristiche soggettive di esperienza, capacità ed affidabilità, elencando analiticamente gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Occorre, poi, redigere un elenco degli amministratori di sistema con indicazione delle funzioni ad essi attribuite (ciò è da farsi anche per i servizi in outsourcing), ed occorre informare i lavoratori del nominativo degli amministratori di sistema aventi accesso a sistemi che trattano dati dei dipendenti. Almeno una volta all'anno l'azienda deve verificare che l'attività svolta dall'amministratore di sistema nell'esercizio delle sue funzioni sia conforme alle mansioni attribuite. Infine, è prescritto l'obbligo di registrare gli accessi logici (autenticazione informatica) ai sistemi di elaborazione ed agli archivi elettronici da parte degli amministratori di sistema, ove per 'access log' si è chiarito che debba intendersi "la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di un amministratore di sistema o all'atto della sua disconnessione", e si è precisato che l'evento che deve essere registrato nel log è solo l'accesso e non anche le attività eseguite. Le registrazioni (access log) devono poi avere carattere di completezza, inalterabilità e possibilità di verifica della loro integrità

adeguate, e contenere i riferimenti temporali e la descrizione dell'evento che le ha generate, nonché essere conservate per un periodo non inferiore a sei mesi.

Laura Agopyan
Avvocato in Milano