# La privacy in Farmacia e nell’ambulatorio medico privato

La privacy dei privati cittadini utenti delle farmacie e dei piccoli ambulatori privati spesso è messa a repentaglio da una gestione non accurata delle regole stabilite dalla normativa al riguardo (D.Lgs 196/2003 – “Codice per la protezione dei dati personali”) e da tutte le buone pratiche di gestione della sicurezza delle informazioni.

I titolari di **farmacie** ed **ambulatori medici** polifunzionali sono di fatto legali rappresentanti di imprese che, seppur di piccole dimensioni, raccolgono e gestiscono **dati personali sensibili** (in particolare dati sanitari relativi alla salute delle persone) di una **grande moltitudine di persone** fisiche e, come tali, sono tenuti a rispondere di fronte alla legge di tali gestioni.

In questi ultimi anni si è passati da una gestione prevalentemente cartacea dei dati personali sensibili raccolti da queste organizzazioni, ad una gestione elettronica di molte informazioni che riguardano la sfera privata delle persone, ovvero i **dati sanitari**.

Se pensiamo ad una farmacia moderna possiamo trovare molti **trattamenti di dati in formato digitale** che solo pochi anni fa non erano presenti: si passa dal ben noto scontrino fiscale parlante (sul quale ha molto disquisito il Garante della Privacy), generato e poi gestito da un sistema informatico, alla ricetta elettronica di recente introduzione, passando per una serie di servizi che le farmacie hanno introdotto da pochi anni: intolleranze alimentari, analisi della pelle, gestione referti esami diagnostici, preparazione di diete, fidelity card, e-commerce, ecc.. Ma anche servizi meno recenti come le prenotazioni di esami tramite CUP ASL o la Dispensazione per Conto vengono gestiti dalle farmacie, attraverso appositi portali dedicati, per conto dei clienti.

Ognuno di questi trattamenti di dati presenta vulnerabilità intrinseche per la sicurezza delle informazioni trasmesse: credenziali di accesso non sufficientemente difficili da individuare, scarsa protezione dei PC e dei Server da attacchi esterni, inadeguata protezione dei medesimi elaboratori in caso di furto e via dicendo.

Come le piccole organizzazioni di altri settori industriali o dei servizi, anche le farmacie non sono dotate di personale esperto nella gestione della sicurezza dei sistemi informatici e spesso il coinvolgimento dei fornitori esterni specializzati non è così sistemato (soprattutto per motivi di costo) da poter garantire una protezione adeguata.

RIPARBELLA C'È STATA ANCHE UNA LITE FRA UN CLIENTE E IL PERSONALE

«Non c'è privacy in farmacia»

– RIPARBELLA – «C'ERANO già state diverse segnalazioni di cittadini infastiditi da una generale mancanza di privacy durante l'acquisto dei medicinali nella farmacia comunale — scrive Alessandro Lucibello Piani della lista civica "Insieme per cambiare» — e come spesso capita l'inerzia nel non cercare un rimedio fa sì che le tensioni si acuiscano ed è di pochi giorni fa il caso di un acceso scontro verbale tra un cliente e gli addetti alla farmacia. Pur considerando la difficoltà di istituire nella piccola farmacia di Riparbella le obbligatorie e appropriate distanze di cortesia per rispettare la privacy dei cittadini resta comunque obbligatorio adottare soluzioni tali da prevenire, durante i colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute dei cittadini. Oltre ad esporre un cartello con la dicitura "Per il rispetto della riservatezza si prega la clientela di attendere il turno a debita distanza" le persone che non sono tenute per legge al segreto professionale non dovrebbero accedere dietro al banco negli orari di apertura, e ora è opportuno che si attivi subito il responsabile comunale intervenendo urgentemente per sensibilizzare tutti sul tema della privacy».

D'altro canto **dai computer delle farmacie transitano quantità di dati sensibili di gran linga superiori a quelle di altre piccole organizzazioni** e costituiscono il canale di consultazione di archivi di prenotazione di esami diagnostici di un elevatissimo numero di pazienti. Da qui la necessità di proteggere i sistemi informatici delle farmacie, sia da un punto di vista logico, sia fisico, in modo molto più attento rispetto ad un normale PC aziendale.

Anche i **piccoli ambulatori privati**, che ospitano medici che eseguono visite specialistiche ed esami diagnostici, ultimamente hanno trovato grande beneficio dall'utilizzo delle nuove tecnologie, nonostante la ritrosia all'utilizzo del computer da parte di numerosi medici. Tutto ciò, però, comporta **la necessità di proteggere adeguatamente i dati sensibili dei pazienti** che transitano in formato digitale in reti locali poco protette. In tali organizzazioni spesso non è nemmeno chiaro chi è il titolare del trattamento dati – il medico che visita il paziente o il centro medico – ed a chi vengono eventualmente delegate le responsabilità per i trattamenti delegati ad altri.

In generale, nelle farmacie e nei piccoli centri medici, tutta la "parte informatica" è delegata a **fornitori specializzati** che talvolta non conoscono in modo preciso la normativa sulla privacy e sono **negligenti nel sottoscrivere le proprie assunzioni di responsabilità** a fronte delle attività eseguite; conseguentemente **tutte le responsabilità ricadono sul titolare del trattamento**, persona fisica o giuridica avente comunque un legale rappresentante, generalmente poco avvezzo a questioni informatiche.

Dal punto di vista normativo, poi, il passaggio da una **normativa italiana** – molto completa e severa per taluni aspetti, ma ormai **obsoleta** per quanto riguarda il **disciplinare tecnico delle misure minime di sicurezza** – ad un nuovo **Regolamento Europeo in fase di approvazione**, non fa che complicare le cose per le piccole organizzazioni che finora hanno avuto regole precise (password di almeno 8 caratteri variate ogni 3 mesi se si trattano dati sensibili, backup almeno ogni 7 giorni, aggiornamenti semestrali dei programmi software, assenza di idonee dichiarazioni di conformità dei fornitori, ecc.) con le quali confrontarsi. Il nuovo Regolamento, infatti, introdurrà la necessità di **valutare i rischi che si corrono dal punto di vista della sicurezza dei dati personali** e, conseguentemente, **progettare il sistema di gestione della privacy** in funzione delle reali esigenze di riservatezza, adottando misure di sicurezza adeguate (non solo "minime").

Inoltre l'attuale versione del Regolamento Europeo sulla Privacy in approvazione contiene l'obbligo per i titolari di dati personali di dotarsi – entro determinate condizioni – di un "***Privacy Officer***", ovvero di una persona, dotata di **adeguate competenze in materia di privacy e sicurezza dei dati**, **responsabile per la gestione**

**della privacy** all'interno dell'organizzazione. Ma il limite attualmente stabilito per l'obbligo di nominare un Privacy Officer è legato al numero di dati personali gestiti (più di 5000 in un anno) che viene facilmente superato da una farmacia di medio volume di affari, ma non da numerose imprese industriali con oltre 50 dipendenti.

La ratio del nuovo Regolamento UE è evidentemente quella di **garantire migliore protezione dove esistono maggiori rischi**, sia per il numero di dati personali trattati, sia per la vulnerabilità dei sistemi.

Il **cambio di mentalità** di chi gestisce **piccole organizzazioni nel settore sanitario** non sarà facile, anche perché non ci saranno più regole precise da seguire per stare tranquilli, ma, oserei dire giustamente, **il Regolamento Europeo ribalterà la responsabilità di progettare un sistema di gestione della privacy adeguato sulle spalle degli imprenditori**. Molti di questi ultimi non saranno in grado di valutare in modo competente ed oggettivo quali misure adottare e dovranno fare attenzione a non credere alle "ricette preconfezionate" a basso costo che hanno già rovinato l'approccio alla privacy negli anni del ben noto **DPS** (Documento Programmatico sulla Sicurezza).

Già oggi il rischio di molte piccole organizzazioni del settore sanitario è quello di non essere conformi alla legislazione attuale sotto diversi aspetti (mancate nomine degli incaricati, mancanza di credenziali di autenticazione ai sistemi informatici adeguate e variate periodicamente, utilizzo troppo invasivo della videosorveglianza, archiviazione di dati privi di protezione, ecc.), figuriamoci domani se saranno i titolari del trattamento (ovvero i legali rappresentanti o direttori delle organizzazioni) a dover **decidere quali misure di sicurezza sono adeguate**! Il rischio concreto è quello di **sottovalutare il problema privacy**, come del resto è avvenuto dopo l'abolizione del DPS che non ha abolito tutti gli altri adempimenti!

Dimenticarsi di proteggere adeguatamente i dati personali dei propri clienti può comportare non solo **sanzioni civili** (e in alcuni casi anche reati penali) in caso di **ispezione da parte del nucleo Privacy della Guardia di Finanza** (oggi peraltro molto rare), ma anche, in caso di **richiesta di risarcimento danni da parte dell'interessato** i cui dati sensibili sono stati violati, ingenti perdite economiche. Talvolta, poi, la mancata diligenza del titolare del trattamento potrebbe portare anche al divieto di intraprendere relazioni commerciali con la Pubblica Amministrazione, riducendo o annullando di fatto la possibilità di operare.

Infine, oltre agli aspetti legati al rispetto della normativa cogente, esistono altri pericoli a cui è sottoposta una organizzazioni che gestisce in modo inconsapevole la sicurezza dei dati, ad esempio la **perdita di dati** e **l'indisponibilità di risorse per garantire la continuità del servizio** al cliente e, quindi, perdite economiche più o meno rilevanti in funzione della gravità

dell'evento.

Altre risorse in rete:

- http://www.federfarmalombardia.it/documents/servizi/vademecum_privacy.pdf
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3533579
- http://www.federprivacy.it/forum/17-privacy-in-campo-sanitario/307-privacy-in-farmacia-e-negli-studi-medici.html
- http://www.federfarma.it/Edicola/Ultime-notizie/17-05-2014-07-30-18.aspx?feed=FederfarmaUltimeNotizie
- http://www.sicurezzamagazine.it/telecamere-nelle-farmacie/
- http://quellichelafarmacia.com/19493/sicurezza-farmacia-abuso-videosorveglianza-una-violazione-privacy/#sthash.RJlzvePR.dpbs

---

# Le novità sulla privacy passate e future


Dall'introduzione del **D.lgs 196/2003**, noto come **Codice sulla Privacy**, sono state introdotte e modificate numerose norme nel settore della protezione dei dati personali e non. Anche il Codice Civile ed il Codice Penale hanno visto numerosi aggiornamenti, per così dire "tecnologici", relativi a comportamenti illeciti e reati perpetrati attraverso gli strumenti informatici e soprattutto via internet.

La legge sulla privacy da un lato si è dovuta adeguare alle nuove situazioni legate alla pubblicazione di altre normative legate al trattamento dei dati personali, dall'altro ha visto, nel giro di pochi mesi, ridursi gli adempimenti delle organizzazioni relativamente alla gestione dei dati personali relativi a persone giuridiche, ai trattamenti per fini amministrativo-contabili ed al decaduto obbligo di redazione ed aggiornamento del **Documento Programmatico sulla Sicurezza** (DPS).

Se escludiamo provvedimenti nati per settori specifici (*data breach* in ambito telco, tracciabilità degli accessi ai dati bancari ), in attesa del **nuovo Regolamento UE sulla privacy** che verrà emesso il prossimo anno a livello di Comunità Europea, gli adempimenti obbligatori per le aziende non sono certo aumentati, anche il **rischio D.Lgs 231** che incombeva su molte organizzazioni, relativo all'introduzione dei reati sulla privacy (trattamento illecito di dati personali), **è stato evitato**. Infatti quanto previsto dal Decreto Legge n. 93/2013 è stato convertito in Legge **eliminando**

**la norma sull'inclusione dei reati privacy nell'elenco dei reati della 231** (la norma prevista dal D.L. 93/2013 non è stata convertita dalla legge 15 ottobre 2013, n. 119 in vigore dal 16 ottobre: il comma 2 dell'articolo 9 del DL 93/2013 è stato soppresso dalla legge di conversione 119/2013; le disposizioni prevedevano l'ingresso tra i "reati presupposto" inclusi nel D.lgs 231/2001 anche dei delitti in materia di privacym non le contravvenzioni, tra cui il trattamento illecito dei dati e le false comunicazioni al Garante).

Da ormai 10 anni a questa parte l'applicazione del codice per la protezione dei dati personali è stata vista dalle varie organizzazioni per lo più come un'incombenza burocratica, che toglie tempo e risorse alle attività cosiddette "produttive". L'unico motivo per cui applicare le misure minime di sicurezza, fornire l'informativa, nominare gli incaricati ed i responsabili del trattamento per molti imprenditori è stato quello di "essere in regola" ed evitare le possibili sanzioni legate al mancato rispetto per la privacy.

La crisi economica e la necessità, o volontà, per molte organizzazioni di ridurre i costi di struttura ha portato a **distogliere risorse dalla compliance privacy**: tagli ai costi per consulenze e servizi di assistenza informatica collegati (ad es. Amministratore di Sistema), meno tempo dedicato ad osservare gli adempimenti previsti, meno formazione del personale, ecc..

Del resto il rischio per l'organizzazione di subire impatti negativi (sanzioni, richieste di risarcimento danni, ecc.) dalla mancata applicazione rigorosa del Codice della Privacy si è via via ridotto a qualche ipotetica ispezione del famoso "Nucleo Privacy della Guardia di Finanza" oppure a denunzie di interessati i quali ritengono che i propri dati personali sono stati trattati in modo illecito.

Occorre anche sottolineare che le "**misure minime di sicurezza**" delineate dal Garante nella prima versione del D.Lgs 196/2003, nell'allegato B, non sono certo **misure adeguate** nel 2013 (si pensi all'aggiornamento dell'*anti-malware* con cadenza semestrale).

Fortunatamente chi ha applicato le misure di sicurezza le ha attuate in modo sostanzialmente corretto (ad es. ogni antivirus prevede un aggiornamento almeno settimanale dei database dei virus), anche se non è raro vedere suite di sicurezza software non configurate in modo adeguato, procedure di backup poco sicure, autenticazioni con password deboli e così via.

Per quanto riguarda il futuro prossimo, il **nuovo Regolamento UE** sarà legge immediatamente in ogni Stato della Comunità Europea ed avrà un significativo impatto sul Codice della Privacy attualmente in vigore in Italia, in quanto le regole sulla protezione dei dati personali dovranno essere necessariamente le stesse in tutti gli Stati membri.

Alcune norme del suddetto Regolamento potranno essere abbastanza pesanti per imprese

ed enti, anche se la versione attualmente in discussione non è ancora definitiva.

Vediamo alcune situazioni esemplificative:

- Viene richiesto maggior dettaglio nell'informativa al trattamento di dati personali (ad esempio l'indicazione del periodo di conservazione dei dati per ogni tipo di trattamento, possibilità di trasferire i dati ad un Paese terzo) ed alla richiesta di consenso (ogni consenso al trattamento deve essere distinguibile da altri tipi di consenso).
- L'esecuzione dei trattamenti su commissione (ovvero *l'outsourcing*, ad es. per il servizio paghe) deve essere disciplinata da un contratto o altro atto giuridico scritto che vincoli il titolare del trattamento al responsabile esterno del trattamento (si precisa che nella dizione originale del regolamento si parla di "incaricato del trattamento" al posto di r"responsabile" e "responsabile del trattamento" al posto di "titolare del trattamento", secondo la dizione italiana vigente).
- Il responsabile esterno al trattamento dei dati personali che tratta i dati conferitigli diversamente dalle istruzioni impartitegli dal titolare diviene titolare egli stesso del trattamento con le conseguenti responsabilità giuridiche.
- Dovranno essere attuati adempimenti molto dettagliati sulla documentazione da conservare relativa ai trattamenti di dati personali, sia per il titolare che per il responsabile del trattamento (non è una documentazione come quella contenuta nel DPS ma si avvicina molto ad esso).
- Le misure di sicurezza adottate dovranno essere appropriate ai rischi che incombono sui dati ed alla natura dei dati trattati; è peraltro richiesta una valutazione dei rischi.
- L'obbligo di comunicazione, sempre, all'Autorità di Controllo (Garante Privacy in Italia) ed agli interessati, quando richiesto, di violazioni di dati personali (*data breach*) incombe su tutti i titolari e responsabili di trattamento e per tutti i tipi di trattamento.
- È richiesta una valutazione dell'impatto del trattamento sulla protezione dei dati personali in caso di trattamenti particolari su cui incombono rischi specifici.
- C'è l'obbligo di nomina di un **responsabile della protezione dei dati** (con un profilo professionale abbastanza definito) per imprese che trattino dati di almeno 500 interessati (in certi settori B2C praticamente tutte le organizzazioni) ed in caso di profilazione dei dati; tale responsabile avrà il compito di garantire il rispetto di requisiti normativi specifici.

Infine il Regolamento fissa le sanzioni amministrative previste, ma non quelle penali la cui definizione è riservata agli Stati membri.

Altri provvedimenti recenti del Garante della Privacy hanno riguardato lo *spam*, o meglio le **comunicazioni commerciali con finalità di marketing** che possono essere indesiderate da chi le riceve e la **privacy nel Condominio** (che aggiunge nuovi

adempimenti per gli Amministratori di Condominio che sono stati recentemente interessati alla Riforma del Condominio).

Infine occorre portare particolare attenzione all'ambito **videosorveglianza e controllo dei lavoratori**, che, sebbene la normativa non sia sostanzialmente cambiata (vedasi art. 4 dello Statuto dei Lavoratori), grazie alla diffusione di nuovi strumenti elettronici (sistemi di sorveglianza sempre più evoluti gestiti da software accessibili anche dal web, *internet content filtering*, sistemi di controllo accessi anche con caratteristiche biometriche quali impronte digitali, log di accessi ai sistemi informatici, ecc.), vede la casistica di possibili violazioni molto più estesa che in passato ed è opportuno consultare le sentenze passate in giudicato per dirimere questioni sempre più complesse. In particolare il giusto equilibrio fra difesa dei diritti dei lavoratori a non essere controllati ed i cosiddetti "controlli difensivi" va comunque valutato di caso in caso, anche in funzione dei possibili illeciti o reati che si vuole prevenire o scoprire.

Linee guida in materia di attività promozionale e contrasto allo spam – 4 luglio 2013 [2542348]

Vademecum – Il condominio e la privacy – versione pagina singola

CloudWatch

---

# Alcune novità nel nuovo provvedimento del Garante della Privacy sulla videosorveglianza

Il recente provvedimento del Garante per la Protezione dei Dati Personali (8 aprile 2010) ha aggiornato le regole precedentemente emanate sulla gestione della videosorveglianza.

Il Garante ha precisato che la raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini fisse o in movimento si configura come trattamento di dati personali. È  considerato dato personale, infatti, qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

Premesso che la videosorveglianza può essere utilizzata senza consenso degli interessati (soggetti ripresi) a fini di sicurezza (prevenzione di reati contro la

persona e la proprietà, sicurezza stradale, ecc.) da enti pubblici e privati, 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, sul controllo a distanza dei lavoratori, in materia di sicurezza presso stadi e impianti sportivi, o con riferimento a musei, biblioteche statali e archivi di Stato, in relazione ad impianti di ripresa sulle navi da passeggeri adibite a viaggi nazionali e, ancora, nell'ambito dei porti, delle stazioni ferroviarie, delle stazioni delle ferrovie metropolitane e nell'ambito delle linee di trasporto urbano. Il tutto puchè venga garantito un corretto bilanciamento di interessi nella videosorveglianza e 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 (ad es. prevenzione di reati o individuazione dei soggetti che li hanno commessi).

Il Garante ha altresì disposto che gli interessati devono essere sempre informati che stanno per accedere in una zona video sorvegliata. 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* in allegato al provvedimento in oggetto e liberamente scaricabile dal sito www.garanteprivacy.it .

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 di videosorveglianza;
- 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 (D.lgs 196/2003), 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).

Se i trattamenti di dati personali sono effettuati da soggetti privati tramite sistemi di videosorveglianza direttamente collegati con le forze di polizia, l'attivazione del predetto collegamento deve essere reso noto agli interessati (che devono dunque essere avvertiti che le riprese sono visionate dalla polizia o dai Carabinieri). 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 – riportato in *fac-simile* in allegato al provvedimento in oggetto ed anch'esso liberamente scaricabile dal sito internet del Garante. Nell'ambito del testo completo di informativa reso eventualmente disponibile agli interessati, tale collegamento deve essere reso noto.

Quando poi 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, i trattamenti di dati personali nell'ambito di una attività di videosorveglianza devono essere effettuati rispettando le misure e gli accorgimenti prescritti dall'Autorità per la Protezione dei Dati Personali come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello del titolare. Ad esempio, devono essere sottoposti alla verifica preliminare del Garante 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.

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 nel provvedimento in oggetto e nel Codice.

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.

Resta inteso che il normale esercizio di un impianto di videosorveglianza, non rientrante nelle ipotesi previste in precedenza, non deve essere sottoposto all'esame preventivo del Garante, sempreché il trattamento medesimo avvenga con modalità conformi al provvedimento del Garante. 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. 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).

È 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. Il Garante ritiene tuttavia necessario che le stesse siano quanto meno rispettose dei principi che seguono:

- in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini. 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 (ovvero, nel caso di sistemi di videosorveglianza guidati da appositi programmi software, essi devono essere dotati di un sistema di autenticazione che permetta di distinguere i differenti accessi);
- 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 ("in diretta"), ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
- 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 (24 ore nella maggior parte dei casi);
- 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 (sarebbe opportuno cautelarsi con apposita dichiarazione sottoscritta dal manutentore);
- 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 (virus informatici e *malware* in genere, attacchi di *hacker*), dunque anche i sistemi software di videosorveglianza dovranno essere protetti da appositi applicativi di sicurezza informatica.;
- 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).*

Il titolare o il responsabile del trattamento dei dati acquisiti dall'impianto di videosorveglianza 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. 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.).

L'omessa adozione delle misure minime di sicurezza non solo comporta l'applicazione della sanzione amministrativa stabilita dal codice, ma integra anche la fattispecie di reato prevista dall'art. 169 del Codice.

Riguardo alla durata dell'eventuale conservazione delle registrazioni, nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità, anche l'eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario – e predeterminato – a raggiungere la finalità perseguita.

La conservazione deve essere, quindi, limitata a poche ore o, al massimo, alle 24 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. Nel caso sia giustificato un più ampio tempo di conservazione dei dati si ritiene che tale periodo non debba comunque superare la settimana.

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 sovraregistrazione, 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. Attenzione agli impianti di videosorveglianza che rilevano solo i movimenti (*motion detection*): durante i periodi di chiusura degli uffici e degli esercizi da proteggere (ad es. durante la notte o durante i giorni di chiusura per festività, ferie, ecc.) tali sistemi potrebbero rilevare immagini riprese in tempi passati ben oltre i limiti consentiti anche se il sistema è programmato per registrare solo 24 ore in quanto la registrazione viene fermata in assenza di movimenti rilevati nell'area sorvegliata.

Deve essere poi 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.

Nell'ambito dei rapporti di lavoro il garante precisa che nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa, pertanto è vietata l'installazione di apparecchiature specificatamente preordinate alla predetta finalità: non devono quindi essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul *badge).* 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 (ad es. per prevenire o rilevare eventuali furti di prodotti): in tali casi, ai sensi dell'art. 4 della I. 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".*

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 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).

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, 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.

Le immagini idonee a rivelare lo stato di salute non devono essere comunque diffuse. In tale quadro, va assolutamente evitato il rischio di diffusione delle immagini di persone malate su *monitor* collocati in locali liberamente accessibili al pubblico.

Riguardo all'utilizzo di web cam o camera-on-line a scopi promozionali-turistici o pubblicitari il Garante ha precisato che 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.

Particolari cautele dovranno poi essere adottate da quelle Società che erogano servizi di videosorveglianza a diverse organizzazioni, al fine di garantire che soltanto i diretti interessati possano accedere alle immagini riprese presso i propri luoghi sorvegliati. Tali società si configureranno come responsabili del trattamento e il 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 precedentemente citato. Tale collegamento deve essere altresì reso noto nell'ambito del testo completo di informativa reso eventualmente disponibile agli interessati.

Le modalità di trattamento sopra elencate richiedono l'adozione di specifiche misure di sicurezza ulteriori rispetto a quelle individuate in precedenza, quali:

- 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;
- 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).

Anche per i soggetti pubblici sussiste l'obbligo di fornire previamente l'informativa agli interessati, *p*ertanto, 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", già citato.

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.

Infine, riguardo al **trattamento di dati personali per fini esclusivamente personali, il Garante ha precisato che l**'installazione di sistemi di videosorveglianza 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. 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 del Codice Penale),* 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.

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.

Il provvedimento in oggetto 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.

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.), restando 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.).

In particolare, per quanto concerne le riprese nelle aree condominiali comuni, qualora i trattamenti siano effettuati dal condominio (anche per il tramite del relativo Amministratore Condominiale), si evidenzia che tale specifica ipotesi è stata recentemente oggetto di una segnalazione da parte del Garante al Governo ed al Parlamento; 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).

Le principali scadenze per l'attuazione delle prescrizioni nuove presenti nel provvedimento del Garante di aprile 2010 sono le seguenti:

- entro dodici mesi, rendere l'informativa visibile anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
- 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;
- entro dodici mesi, adottare, le misure di sicurezza a protezione dei dati registrati tramite impianti di videosorveglianza;
- entro sei mesi, adottare le misure necessarie per garantire il rispetto di quanto indicato nel provvedimento per quanto concerne i sistemi integrati di videosorveglianza.