

Articoli Privacy in Ambito Sanitario

28 marzo 2005 - Sieropositivi: particolari garanzie a tutela dei loro dati

Gli articoli di stampa riguardanti persone sieropositive devono rispettare particolari garanzie volte a prevenire l'ingiustificata diffusione di dati personali, come quelli relativi alle foto degli interessati. Anche in caso di diffusione di dati a margine di fatti all'attenzione della magistratura penale, qualora sussista la necessità di "allertare" persone che hanno avuto rapporti con soggetti sieropositivi, le forze di polizia devono adottare modalità rispettose della dignità e della riservatezza degli interessati.

Intervenendo a seguito di una segnalazione della Lila (Lega italiana per la lotta contro l'Aids), l'Ufficio del Garante ha invitato l'editore di un quotidiano a non pubblicare più, spontaneamente, la foto che ritraeva un giovane sieropositivo arrestato per altri fatti, ma sottoposto ad indagine per possibili lesioni nei confronti di alcune donne. Il quotidiano ha aderito spontaneamente alla richiesta dell'Autorità ed ha interrotto l'ulteriore diffusione dell'immagine.

Ribadendo quanto già affermato a suo tempo per un caso analogo, l'Autorità ha richiamato l'attenzione sul fatto che la pubblicazione di foto riguardanti persone affette da virus Hiv può, in casi del genere, violare i principi sanciti dalla disciplina sulla protezione dei dati e dal [codice di deontologia per l'attività giornalistica](#).

In particolare, l'Ufficio del Garante ha ricordato che si possono individuare modalità di informazione del pubblico assai più selettive rispetto alla divulgazione della fotografia e delle generalità dell'interessato, fornendo, cioè, elementi di informazione indiretti che permettano di raggiungere egualmente lo scopo di informativa prefissato (i luoghi frequentati, il periodo temporale di riferimento). In tal modo, è ugualmente possibile mettere in guardia persone che avrebbero potuto avere contatti con l'interessato (mettendo a disposizione, ad esempio, informazioni più dettagliate attraverso numeri verdi o altri servizi di informazione e assistenza) evitando, al tempo stesso l'esposizione della persona sieropositiva ad una sproporzionata evidenza della propria immagine sui mezzi di informazione.

L'Autorità ha anche ricordato come la necessità di assicurare la doverosa tutela della dignità e della riservatezza alle persone sieropositive e l'obbligo di astenersi dalla diffusione di dati personali ed immagini da parte delle forze di polizia, siano stati oggetto di due circolari del Ministero dell'interno (27 novembre 2003 e 26 febbraio 1999) e di una circolare del Comando generale della Guardia di finanza (19 gennaio 2004).

La stessa recente sentenza della Corte europea dei diritti dell'uomo, dell'11 gennaio 2005, riguardante un caso italiano di diffusione di dati a seguito di conferenze stampa tenute da organi inquirenti, ha confermato inoltre il quadro di rigorose garanzie previste nella normativa italiana.

21 febbraio 2005 - Telemedicina, telelavoro e diritti delle persone

"Nei processi di automazione della sanità pubblica dovranno rientrare anche le regole previste per la protezione dei dati personali".

Lo ha affermato Gaetano Rasi, componente dell'Autorità Garante per la protezione dei dati personali, in occasione della presentazione del libro "I processi di automazione nella sanità pubblica, telelavoro e telemedicina: attualità e prospettive" di Fabio Massimo Gallo e Carlo Parasceni, svoltasi il 23 febbraio scorso.

Le applicazioni di telemedicina - ha ricordato Rasi - risultano sempre più diffuse nel mondo ed in costante aumento in Europa. In Italia il 40% delle strutture mediche che si avvalgono delle innovazioni tecnologiche utilizza il televideoconsulto e quasi il 25% soluzioni dedicate all'home care. La telemedicina offre nuove opportunità di collegamento tra punti diversi sul territorio e costituisce un valido ed efficace strumento di interconnessione tra i diversi livelli di cura per giungere alla continuità della diagnostica e della terapia, indipendentemente da dove il paziente o le informazioni risiedono. Attraverso la creazione di una rete telematica di strutture sanitarie è possibile, infatti, ottenere informazioni sulla disponibilità di posti letto, sull'accesso alle liste di prenotazione, sulla gestione delle cartelle cliniche con gli adeguati accorgimenti per la tutela della privacy.

È necessario, tuttavia, quanto più si sviluppano le reti telematiche, fissare precise regole per garantire il rispetto della dignità della persona e la massima riservatezza dei dati personali, in particolare, di quelli sensibili, così qualificati perché idonei a rivelare gli aspetti più intimi e riservati della persona, nel cui ambito rientrano le informazioni relative allo stato di salute.

Anche l'outsourcing e il telelavoro - ha osservato poi il componente dell'Autorità - sono realtà in espansione e contribuiscono alla profittabilità del business e all'efficienza delle pubbliche prestazioni. Il 43% dei contratti di outsourcing copre, ad esempio, l'area dell'Information technology, il 25% quella delle risorse umane. In quest'ultimo caso vengono affidati a partner esterni non solo l'amministrazione, ma anche, per esempio, la gestione del percorso di carriera dei dipendenti.

Secondo il segretario generale del Garante, Giovanni Buttarelli, intervenuto anch'egli alla presentazione, l'euforia informatica pone nuovi rischi, ma il codice della privacy rappresenta uno strumento importante di tutela.

"L'euforia informatica - ha dichiarato Buttarelli - non deve far dimenticare che Costituzione Europea e Codice della Privacy mettono in primo piano il diritto della persona a verificare come vengono trattati i propri dati personali. Siamo forse primi nel

mondo per il quadro giuridico sull'informatica e la telematica. Il Testo Unico sulla privacy è pronto per rispondere alle questioni poste dalla telemedicina, che recherà grossi vantaggi, come la possibilità di accedere con una password alla propria cartella clinica da qualunque parte del mondo, ma causerà anche nuovi rischi relativi, ad esempio, alla dispersione di informazioni. L'informatica al cittadino dovrà tenere conto di tutti questi aspetti".

Il percorso di informatizzazione della Pubblica Amministrazione - ha proseguito il segretario generale dell'Autorità - ha portato dalla rete unitaria della PA alla rete degli uffici di gabinetto, passando poi con la telematica all'e-governement ed al d-governement con l'avvento del digitale. Tanti i temi su cui le innovazioni vanno ad incidere: protocolli informatici, interoperabilità dei sistemi, tessera sanitaria, outsourcing. I rischi possono essere di vario tipo. Innanzitutto riguardano quello che potremmo definire health divide, cioè proprio i soggetti che necessitano di maggiore tutela, come anziani, portatori di handicap, possono venire esclusi da un'amministrazione digitale. Inoltre, l'automazione o la telematizzazione permettono di superare alcuni problemi relativi alla privacy, quali le distanze di cortesia o la promiscuità, ma ne possono creare di nuovi relativi ad esempio alla circolazione dei dati. e alla sicurezza.

La terza categoria di rischi è inerente al regional divide. Le maggiori competenze in materia da parte delle Regioni, che stanno provocando anche l'intervento della Corte Costituzionale, potrebbero portare a disparità di trattamento basate sulle differenti "velocità".

Sulle nuove "autostrade del sole" del trattamento dei dati - ha concluso Buttarelli - il cittadino avrà sempre il diritto di intervenire sul trattamento dei propri dati.

3 gennaio 2005 - Anche le foto scattate a fini di interventi chirurgici sono dati personali

Una donna ottiene le fotografie dell'operazione di chirurgia plastica grazie all'intervento del Garante

Si rivolge al Garante e riesce ad ottenere le fotografie scattate prima e dopo alcuni interventi di chirurgia plastica ai quali si era sottoposta e che intendeva produrre in una causa di risarcimento danni nei confronti del medico che l'aveva operata.

Protagonista una giovane donna che dal 1996 al 2003 aveva subito tre interventi chirurgici al seno per impianti di protesi, successive sostituzioni e riduzione delle cicatrici. Palesemente insoddisfatta dei risultati raggiunti, nel tentativo di recuperare tutta la documentazione clinica che la riguardava, aveva chiesto direttamente al chirurgo plastico al quale si era affidata le foto che lo stesso le aveva scattate prima e dopo le operazioni e copia dei moduli di consenso agli interventi, sottoscritti presso lo studio medico. Di questa documentazione non vi era traccia nella copie delle cartelle cliniche rilasciate alla paziente dalla casa di cura presso la quale aveva subito gli interventi. Di fronte all'assoluto silenzio del medico, la donna si è vista "costretta" a presentare ricorso al Garante. Iniziativa che si è rivelata di per sé sufficiente a farle raggiungere l'obiettivo.

Già nella fase di primo esame del procedimento, infatti, il medico, seppure su invito dell'Autorità, ha dato completo riscontro alle richieste della paziente. Il ricorso è stato quindi definito con provvedimento di non luogo a provvedere.

Il Garante ha comunque posto a carico del chirurgo plastico le spese del procedimento, per aver concesso alla donna l'accesso ai propri dati solo dopo la presentazione del ricorso. La richiesta presentata al medico era, infatti, pienamente legittima, essendo stata presentata ai sensi del Codice, che riconosce ad ognuno il diritto di accedere a tutti i propri dati personali, comprese le fotografie che ritraggono in tutto o in parte il proprio corpo.

3 gennaio 2005 - Sanità e protezione dei dati

Giornata di approfondimento organizzata dal Garante sull'applicazione del Codice presso le strutture sanitarie pubbliche e private

Nell'ambito dell'attività di formazione svolta dal Garante, il 2 febbraio si terrà un incontro di approfondimento su alcune significative esperienze maturate presso organismi sanitari pubblici e privati che hanno attuato le disposizioni del Codice nel settore della sanità sulla base di soluzioni idonee ed in alcuni casi innovative, adottate con modalità rispettose dei principi di semplificazione, armonizzazione ed efficacia.

Principale obiettivo dell'iniziativa, che avrà come prevalenti relatori gli operatori degli organismi sanitari, è quello di illustrare le concrete modalità di realizzazione delle misure adottate per garantire nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati.

Sulla base delle più significative esperienze maturate da taluni organismi sanitari, avvalendosi anche di un confronto dialettico con il Garante, sarà possibile offrire una gamma di modelli operativi, utili alle varie realtà sanitarie chiamate ad applicare le disposizioni del Codice.

Gli organismi sanitari che hanno delineato percorsi organizzativi che si distinguono per innovatività, semplicità, efficacia - specie in riferimento alle varie prestazioni erogate da distinti reparti ed unità di uno stesso organismo o da più strutture ospedaliere o territoriali - sono invitate a far pervenire all'Autorità, prima dell'incontro, una breve descrizione di tali iniziative realizzate (indirizzare unicamente alla casella di posta elettronica sitoweb@garanteprivacy.it).

L'Autorità si riserva di selezionare quelle ritenute più significative al fine di favorirne l'illustrazione nell'ambito della giornata di approfondimento.

Le iscrizioni per partecipare all'incontro potranno essere effettuate a partire dal 15 gennaio 2005, secondo le modalità che saranno precisate nei prossimi giorni.

22 novembre 2004 - Familiari spiati nelle camere ardenti. Interviene il Garante

Il sistema di videosorveglianza è stato poi bloccato dallo stesso Comune che lo aveva installato

Familiari e amici che vegliano i defunti spiati, ignari, da telecamere nelle camere ardenti. È successo in Toscana dove gli ispettori del Garante hanno scoperto l'installazione di telecamere "camuffate" che violavano la riservatezza dei familiari e di quanti avevano accesso ai locali dove è ragionevole aspettarsi intimità e rispetto.

Gli accertamenti, effettuati nell'ambito di un ciclo di ispezioni per verificare il rispetto delle regole in materia di videosorveglianza, disposte dal Garante con il provvedimento generale del 29 aprile 2004, hanno consentito di rilevare che gli uffici comunali avevano dotato di telecamere a circuito chiuso, che registravano immagini, l'edificio all'interno del quale vengono allestite camere ardenti per la veglia dei defunti. Le immagini venivano conservate per 15 giorni. L'attività ispettiva ha permesso di "scoprire" la presenza di ben 32 telecamere alcune delle quali erano state installate anche all'interno delle stesse camere ardenti in modo che fossero celate alla vista del pubblico. Il sistema di videosorveglianza non era segnalato ai cittadini mediante le informative necessarie previste dal Codice in materia di protezione dei dati personali.

Agli ispettori del Garante il comune ha spiegato che l'attivazione del sistema era stata originariamente ordinata in relazione ad alcuni episodi di danneggiamento avvenuti anni fa a danno di alcune salme. Alla luce degli accertamenti, il Garante ha verificato che l'installazione non rispettava le norme sulla privacy ed ha invitato il comune ad attuare spontaneamente il "blocco" dei trattamenti svolti mediante il sistema di telecamere, in modo da prevenire un provvedimento analogo dell'Autorità.

In particolare, il Garante ha rilevato che la misura risultava sproporzionata rispetto agli scopi che si intendevano perseguire e che gli stessi tempi di conservazione delle immagini erano eccessivi rispetto a tali scopi.

Il blocco disposto ha comportato l'immediata sospensione di tutte le attività di trattamento dei dati personali, ad eccezione della mera conservazione. In base all'art. 143 del Codice, il titolare, su invito dell'Autorità formulato prima della definizione del procedimento, può infatti sospendere spontaneamente le attività di trattamento.

Il comune ha aderito all'invito e ha preferito sospendere esso stesso le attività di video-sorveglianza presso l'edificio, in attesa che il Garante si esprima sulla complessiva liceità dei trattamenti svolti ed applichi le eventuali sanzioni.

22 novembre 2004 - Accesso non autorizzato al fascicolo personale

Due dipendenti di una p.a. hanno utilizzato illecitamente per fini personali i dati sulla salute di un altro collega e di un suo familiare

Un nuovo, grave episodio di trattamento illecito delle informazioni sulla salute di un dipendente pubblico e di un suo familiare. L'Autorità ha ordinato all'amministrazione di adottare ogni misura di sicurezza per impedire il ripetersi di gravi atti lesivi della riservatezza, e di fornire idonee disposizioni al personale. Gli atti sono stati trasmessi, come d'obbligo nei casi di uso illecito di dati sulla salute, alla magistratura.

A sollevare la vicenda è stato un funzionario in servizio presso una questura che contestava la divulgazione di informazioni sulla sua salute e di quella di sua madre, conservate nel proprio fascicolo personale, avvenuta anche tramite una lettera inviata ad alcuni dirigenti da parte di altre due dipendenti dello stesso ufficio.

Nella lettera, secondo il dipendente, erano riportati, virgolettati, frasi e dettagli relativi a permessi di cui si contestava la legittimità, usufruiti per assistere la madre handicappata; si formulavano poi critiche su alcune prestazioni lavorative. Il funzionario, insoddisfatto della risposta ricevuta dalla questura alla quale si era rivolta contestando quanto successo, ha presentato ricorso al Garante. In questa sede, ha ribadito le proprie richieste chiedendo la cancellazione della lettera dal protocollo dell'archivio del personale, perché i dati in essa contenuti sarebbero stati raccolti in violazione di legge, e di porre fine al trattamento illecito dei suoi dati personali. Nel ricorso si sottolineava anche il grave danno derivato dal fatto che le due dipendenti avessero potuto accedere liberamente senza autorizzazione e senza motivo al suo fascicolo personale. L'amministrazione a giustificazione del suo operato, affermava dal canto suo che già dal 2001 aveva dato disposizioni per l'organizzazione del lavoro d'archivio e che la lettera non è stata mai inserita nel fascicolo dell'archivio, ma è stata trattenuta dal dirigente incaricato di verificarne il contenuto. La questura comunicava, inoltre, di aver interessato dell'accaduto la Procura della Repubblica.

Il Garante ha accolto il ricorso del dipendente ed ha ordinato all'amministrazione di adottare ogni idonea misura di sicurezza per evitare il ripetersi di episodi analoghi. Dalla documentazione è emerso, infatti, che le due dipendenti hanno trattato in modo illecito dati personali e sulla salute del funzionario e della madre, utilizzandoli per formulare proprie rimostranze all'amministrazione. Una delle due non era neanche autorizzata ad avere accesso ai fascicoli dei dipendenti, mentre l'altra,

seppure autorizzata, ha utilizzato indebitamente i dati per fini personali diversi da quelli di servizio. È risultata inammissibile, invece, la richiesta dell'interessato di cancellazione della lettera.

Dopo l'entrata in vigore del Codice, chi effettua un trattamento illecito dei dati personali, specie se sensibili, rischia la reclusione da sei mesi a tre anni, mentre, per mancata adozione delle misure di sicurezza, si può essere puniti con l'arresto fino a due anni o con una ammenda fino a cinquantamila euro.

22 novembre 2004 - Rasi: sui dati biometrici massimo livello di attenzione

"In materia di dati biometrici occorre mantenere alto il livello di attenzione. Il Garante è consapevole dei benefici derivanti dal loro impiego, ma allo stesso tempo vigila per evitare che un loro utilizzo distorto ed eccessivo possa limitare i diritti e le libertà dei cittadini".

Lo ha affermato Gaetano Rasi, componente dell'Autorità Garante per la protezione dei dati personali, al convegno organizzato dal Cnipa sul tema "La biometria entra nell'e-government".

Rasi ha osservato come le informazioni biometriche, cioè le impronte digitali, l'iride, il riconoscimento facciale, per i loro stessi caratteri di universalità, permanenza e unicità, possono rivelarsi utili soprattutto a fini investigativi e di identificazione. Tuttavia le legittime finalità per le quali vengono utilizzate le tecniche biometriche, devono essere bilanciate da adeguate garanzie per i diritti e le libertà delle persone. È accertata, infatti, l'esistenza di falsi positivi e la possibilità che siano compiuti errori o "furti di identità".

Il Codice in materia di dati personali, pur non introducendo una disciplina specifica per i dati biometrici, prevede che il loro trattamento venga comunicato al Garante, al quale è affidato anche il compito di una verifica preliminare per valutare gli interessi in gioco e stabilire cautele speciali per l'uso di informazioni così delicate. E ciò anche nel rispetto dei principi stabiliti a livello europeo dal gruppo che riunisce le autorità per la privacy dell'Ue.

Il Garante italiano - ha ricordato il componente dell'Autorità - ha già affrontato in diversi casi l'uso delle impronte digitali e dei sistemi biometrici, sia da parte di soggetti pubblici che privati, valutando ogni volta la loro reale necessità rispetto agli scopi che si intendono perseguire, e verificando le modalità di rilevazione e registrazione dei dati, i tempi di conservazione, le misure di sicurezza adottate e le modalità di consultazione delle informazioni da parte dei soggetti autorizzati.

In un panorama che vede la biometria come un settore innovativo ed in continua evoluzione - ha concluso Rasi - la disciplina sulla protezione dei dati personali è "imprescindibile", non solo perché da essa si possono ricavare precisi principi affinché la raccolta di dati biometrici sia effettuata in modo lecito, ma anche perché solo il rispetto di queste norme può garantire l'efficienza degli stessi sistemi di raccolta di informazioni ed evitare che esse "si disperdano in disordinati, quanto inutili, database".

[Comunicato stampa del 23 novembre 2004]

15 novembre 2004 - Sanzioni a 11 Asl per trattamenti non trasparenti

Dalle ispezioni del Garante sono emersi vari trattamenti di dati genetici e sulla salute che le strutture non avevano comunicato all'Autorità

Sedici sanzioni amministrative già contestate per omessa o ritardata notificazione di trattamenti di dati particolarmente delicati, al termine di un nuovo ciclo di ispezioni disposte dall'Autorità e curato dal Nucleo funzione pubblica e privacy della Guardia di finanza nei confronti di aziende sanitarie locali, laboratori di analisi e società di lavoro interinale. Alcuni provvedimenti di blocco del trattamento sono in fase di adozione affinché i trattamenti di dati non proseguano fino a quando non saranno regolarizzati. Le contestazioni potrebbero aumentare perché per altri casi si stanno ancora svolgendo accertamenti.

Entro il 30 aprile 2004, tutte le società e gli organismi pubblici che effettuano trattamenti di dati genetici, biometrici, dati sullo stato di salute, sulla vita sessuale, sulle adesioni politiche, convinzioni religiose, etnia, avrebbero dovuto inoltrare al Garante, per via telematica, la notifica di tali trattamenti. Chi non ha provveduto agli adempimenti che il Codice prescrive al fine di trasparenza nei confronti degli interessati rischia di essere sanzionato anzitutto con il pagamento di una somma che va da un minimo di diecimila a sessanta mila euro e con la pubblicazione su uno o più giornali del provvedimento. La notificazione al Garante, infatti, non è una "mera formalità", ma un preciso obbligo.

L'opera di semplificazione degli adempimenti introdotta dal Codice sulla protezione dei dati personali in vigore dal primo gennaio 2004, ha ristretto la notificazione all'Autorità ai soli casi delicati espressamente indicati nel Codice e desumibili anche dal [provvedimento di esonero del Garante del 31 marzo scorso](#). I casi in esame dovevano essere però notificati, trattandosi di trattamenti di dati particolarmente delicati. Più della metà delle trenta società sottoposte a verifiche non sono risultate invece in regola con la normativa. Si tratta in prevalenza di Asl, (11 sulle dodici controllate), di laboratori di analisi (3 sui tre controllati), di una società di lavoro interinale e di una banca.

Altre conseguenze potranno derivare dall'inutilizzabilità dei dati trattati in violazione di legge disposta dal codice. L'attività ispettiva, disposta dal Garante nei confronti di alcune categorie di soggetti che per il tipo di attività svolta potrebbero effettuare trattamenti di dati per i quali è richiesta la notificazione, è stata delegata al Nucleo funzione pubblica e privacy della Guardia di finanza - unità specializzata che collabora con l'Autorità - che ha eseguito gli accertamenti presso le varie società ed ha proceduto alla contestazione diretta delle sanzioni amministrative nei casi in cui sono state rilevate violazioni.

Le società che hanno ricevuto la contestazione possono peraltro avvalersi della possibilità dell'oblazione, prevista dalla legge, versando il doppio del minimo della sanzione pari a ventimila euro, estinguendo in questo modo l'illecito amministrativo, oppure contestarla inviando memorie difensive al Garante. In questo ultimo caso, però, se l'Autorità ritiene comunque fondato l'accertamento determina la somma dovuta per la violazione e ne ingiunge il pagamento insieme con le spese. Resta comunque ferma la necessità che i trattamenti siano pienamente regolarizzati per essere proseguiti.

Ulteriori ispezioni sulla notificazione sono in programma nei prossimi mesi.

18 ottobre 2004 - Dati sanitari in busta chiusa

Risultati della visita medica sotto gli sguardi di tutti. Il Garante dà ragione ad un dipendente comunale

Si sottopone ad accertamenti sanitari per il riconoscimento di infermità da causa di servizio e i referti gli vengono comunicati, tramite il messo comunale, dall'amministrazione di appartenenza spillati ad una nota di accompagnamento, anziché custoditi in busta chiusa.

È successo ad un dipendente comunale che, indignato dall'accaduto ritenuto lesivo della sua riservatezza, dopo una prima istanza rivolta al datore di lavoro in cui chiedeva conto di questa procedura, insoddisfatto della risposta ricevuta, ha presentato ricorso al Garante. L'Autorità gli ha dato ragione ed ha ordinato all'ente locale di conformarsi al rispetto della normativa in materia di protezione dei dati personali. Entro la fine di novembre il comune dovrà comunicare al Garante misure di sicurezza, istruzioni al personale, procedure adottate per la tutela dei dati.

Quando le amministrazioni pubbliche trattano informazioni personali, a maggior ragione se vi sono riferimenti alla salute, alla vita sessuale, alle convinzioni religiose ecc., hanno l'obbligo di adottare ogni cautela e precauzione per prevenire violazioni dei diritti, delle libertà fondamentali e della dignità degli interessati. Dati sanitari, quindi, in busta chiusa e allegati alle note di trasmissione solo se indispensabili.

Nel caso in esame il Garante ha ritenuto illecite sia le modalità di circolazione dei dati all'interno dell'ente (redazione di documenti, invio di note, loro protocollazione), sia quelle di comunicazione all'interessato ed ha richiamato l'amministrazione all'adozione di soluzioni che permettano di svolgere le funzioni istituzionali eliminando ogni occasione di superflua conoscibilità dei dati sulla salute, anche da parte degli incaricati del trattamento, compresi i messi notificatori (dati sanitari in busta chiusa, inviti a ritirare personalmente un documento presso l'ufficio competente, comunicazione telematica direttamente all'interessato). Contrariamente a quanto sostenuto dal Comune, infatti, nelle note recapitate all'interessato erano presenti riferimenti a procedure per il riconoscimento di patologie contratte in servizio, e a esami clinici ai quali il dipendente doveva sottoporsi: tutti dati idonei a rivelare lo stato di salute secondo quanto previsto dal Codice in materia di protezione dei dati personali.

11 ottobre 2004 - Lavoro. Il fascicolo del dipendente è riservato, solo copie autorizzate

Il Garante interviene contro l'indebita diffusione di una lettera contenente dati personali di una lavoratrice e di sua figlia disabile

I datori di lavoro pubblici e privati devono trattare e conservare i dati dei loro dipendenti nel rispetto del diritto alla protezione dei dati, adottando anche, a pena di sanzioni civili e penali, ogni idonea misura di sicurezza per prevenire eventi lesivi della privacy. A maggior ragione se tra le informazioni raccolte compaiono dati sensibili riferiti ad un minore.

Lo ha sottolineato il Garante accogliendo il ricorso di una dipendente di una società che lamentava una grave violazione della propria riservatezza personale e familiare. I fatti risalgono a dicembre dello scorso anno quando la donna, che occupava temporaneamente la scrivania di un collega, alzando una cartellina aveva trovato la fotocopia di una lettera da lei stessa inviata al direttore dell'ufficio, nella quale erano riportate anche delicate informazioni sulla condizione di salute della figlia minore disabile. Per due volte si era rivolta all'amministrazione contestando l'indebita divulgazione della lettera e chiedendo che tale condotta illegittima non venisse a ripetersi. L'interessata chiedeva anche di conoscere in base a quale norma di legge la lettera fosse stata conosciuta da terzi, addirittura in fotocopia, nonché di avere conferma dell'esistenza di dati personali in possesso della società e la loro comunicazione in modo chiaro e dettagliato.

Non avendo ricevuto una adeguata risposta per iscritto ha sottoposto il caso al Garante. L'Autorità ha riconosciuto le ragioni della dipendente e ha ordinato alla società di astenersi dall'ulteriore trattamento illecito dei dati personali dell'interessata. Alla società è stato anche imposto di adottare tutte le misure di sicurezza idonee a prevenire il ripetersi di eventi del genere. Secondo il Garante la presenza ingiustificata di tale fotocopia contenente dati sensibili della dipendente e della figlia minore, al di fuori del fascicolo personale e comunque in un contesto non appropriato, contrasta con la disciplina sulla protezione dei dati personali ed in particolare con le prescrizioni e le cautele indicate nell'autorizzazione generale che disciplina il trattamento dei dati sensibili nei rapporti di lavoro e con le disposizioni in materia di misure di sicurezza. Va ricordato, peraltro, che i dati sensibili devono essere conservati in una sezione separata del fascicolo personale ed essere accessibili solo al personale autorizzato.

La società, che non ha contestato la ricostruzione della vicenda fatta dalla dipendente, ha avviato una indagine interna, non ancora conclusa, i cui esiti dovranno essere comunicati al Garante per la valutazione di altre eventuali violazioni e determinazioni di competenza.

La società dovrà anche far conoscere al Garante le misure di sicurezza adottate e le disposizioni impartite al personale per una doverosa protezione dei dati. Alla società sono state infine addebitate le spese del procedimento da rifondere direttamente alla dipendente.

20 settembre 2004 - Analisi cliniche in strada: accertamenti del Garante

Gli ispettori del Garante per la protezione dei dati personali, in collaborazione con il Nucleo Speciale Funzione Pubblica e Privacy della Guardia di Finanza, si sono recati oggi presso la Asl Roma C per effettuare accertamenti in merito all'episodio delle analisi cliniche abbandonate accanto ai cassonetti, segnalato nei giorni scorsi da alcune notizie di stampa.

Le verifiche degli ispettori vertono sul rispetto delle disposizioni in materia di protezione dei dati personali, in particolare sull'adozione di misure di sicurezza a salvaguardia di dati tanto delicati come quelli sanitari, e sulle responsabilità che dovessero emergere.

Già ieri il Garante aveva effettuato un sopralluogo nella via dove erano stati ritrovati i risultati clinici abbandonati, verificando che essi erano stati parzialmente rimossi.

[Comunicato stampa del 24 settembre]

26 luglio 2004 - Militari in malattia e accessi alle caserme

Informazioni sulla salute non indispensabili. Il Garante interrompe il trattamento dei dati

Con un provvedimento adottato nei confronti del Comando regionale di una forza di polizia il Garante ha vietato un illecito trattamento di informazioni sulla salute di alcuni militari. Al Comando è stato imposto di interrompere ogni operazione e di limitarsi alla sola conservazione dei dati.

Lo ha stabilito il Garante accogliendo i ricorsi di alcuni sottufficiali che lamentavano una violazione della privacy ogni volta che, in licenza per malattia o in aspettativa, recandosi in caserma trovavano all'ingresso un elenco con i nomi di tutti i militari corredate dalle varie cause dell'assenza. In particolare, accanto ai nominativi dei militari temporaneamente assenti dal servizio che l'amministrazione comunica al responsabile che disciplina gli ingressi in caserma, compariva la dicitura "in convalida" o "in aspettativa". Queste informazioni, anche senza l'indicazione di particolari patologie, sono in grado di rivelare lo stato di salute. Per lo scopo perseguito è sufficiente un elenco con i nominativi privo di altre indicazioni.

Dopo una prima istanza rivolta all'amministrazione nella quale si contestava la presenza di tali diciture che a parere dei sottufficiali costituiscono un illecito trattamento di dati sulla salute, insoddisfatti della risposta ricevuta, hanno presentato separati ricorsi al Garante. I militari non contestavano le misure di sicurezza, ma si opponevano al tipo di procedura adottata dall'amministrazione ritenuta lesiva della privacy chiedendone l'interruzione.

Il Garante ha dato loro ragione e ha, dunque, disposto l'interruzione del trattamento illegittimo dei dati.

Contrariamente a quanto sostenuto dal Comando regionale, infatti, l'indicazione del dato relativo all'assenza per "convalida" dà luogo ad un trattamento di dati sensibili dal momento che questa informazione è come detto in grado di rivelare lo stato di salute del dipendente e non risulta, peraltro, indispensabile. Con l'introduzione del nuovo Codice i soggetti pubblici per svolgere attività istituzionali devono poi rispettare il principio di necessità: devono, cioè, impiegare solo dati indispensabili, riducendo al minimo l'utilizzazione di dati personali ed identificativi quando le finalità perseguite possono essere altrimenti raggiunte, come nel caso in esame. Per disciplinare l'ingresso dei militari che si assentano dal servizio è sufficiente indicare solo i loro nomi, senza menzionare espressamente la ragione di tale assenza attinente allo stato di salute. Ed anche se l'amministrazione non ha ancora adottato un regolamento in cui specificare i tipi di dati trattati, le operazioni eseguibili, le finalità perseguite, essa deve comunque attenersi a tale principio, altrimenti il trattamento è illecito.

10 maggio 2004 - Malattie professionali e privacy dei lavoratori

Nelle denunce all'Inail vanno comunicate solo informazioni indispensabili. Il Garante blocca l'uso dei dati sanitari da parte di una p.a.

Nelle denunce di malattia professionale che i datori di lavoro devono trasmettere all'Inail vanno indicate solo informazioni sanitarie relative o collegate alla patologia denunciata e non dati sulla salute inerenti a semplici malesseri accusati o ad assenze registrate nel corso del rapporto di lavoro, non rilevanti per la malattia professionale. Anche se l'amministrazione viene a conoscenza di altri dati, deve comunicare e conservare solo quelli necessari prescritti dalla normativa.

I principi sono stati ribaditi dal Garante (Stefano Rodotà, Giuseppe Santaniello, Gaetano Rasi, Mauro Paissan) in un provvedimento con il quale ha vietato all'Inail di utilizzare i dati sanitari di un'assicurata e ha disposto il blocco di alcune informazioni relative allo stato di salute presenti negli archivi del datore di lavoro e ricavabili dalle diagnosi contenute nei certificati dei lavoratori. All'amministrazione è stato, inoltre, imposto di adottare opportuni accorgimenti per non rendere visibili le diagnosi sulle certificazioni sanitarie detenute.

Al blocco dei dati si è giunti a seguito di una segnalazione di una dipendente che lamentava un trattamento illegittimo di informazioni sanitarie nel corso della procedura avviata per il riconoscimento di malattia professionale. La misura adottata dal Garante si è resa necessaria per evitare il rischio concreto di un pregiudizio per la segnalante e per tutti gli altri lavoratori i cui dati sanitari sono ricavabili dalle diagnosi riportate sui certificati.

L'attuale disciplina in materia prevede, infatti, che il lavoratore assente per malattia sia tenuto a presentare al datore di lavoro solo l'attestazione della prognosi. Può capitare, però, che nel certificato venga indicata anche la diagnosi: in questo caso l'amministrazione, che non è legittimata a trattare questi dati, deve quindi adoperarsi per oscurare la diagnosi e adottare opportuni accorgimenti anche verso lavoratori e medici.

L'amministrazione pubblica presso la quale lavora la segnalante, anziché inviare all'Inail, come prescrive la normativa, solo la denuncia di malattia professionale corredata dal certificato medico con la sintomatologia accusata, aveva invece trasmesso tutti i certificati presentati dalla dipendente nel corso del rapporto di lavoro. Nella documentazione erano presenti più di 60 certificati prodotti dal 1985 al 2000 e una nota riepilogativa delle assenze. Erano oltretutto riportate anche le diagnosi relative a malesseri temporanei (stato febbrile, faringite) e patologie che non risultavano collegabili a quella denunciata all'Inail. La trasmissione di questi certificati medici, ha stabilito il Garante, non è giustificata da alcuna disposizione normativa ed è risultata soprattutto in contrasto con la normativa sulla privacy. Si è verificata, quindi, un'illegittima comunicazione di dati non pertinenti ed ecdedenti ai fini del riconoscimento della malattia professionale e questi dati non potranno essere utilizzati dall'Inail per la valutazione.

Il Garante ha ritenuto necessario disporre ulteriori accertamenti nei confronti dell'amministrazione pubblica che ha comunicato i dati. Copia del provvedimento è stata trasmessa alla magistratura penale per le valutazioni di competenza, perché nel corso del procedimento avviato dal Garante l'amministrazione aveva inoltre negato di aver mai inviato certificati all'Inail.

9 febbraio 2004 - Cartelle cliniche abbandonate. Interviene il Garante

Il Garante è intervenuto sul caso segnalato nella puntata del 10 febbraio da "Striscia la notizia", della struttura sanitaria di S. Maria di Leuca, dove sono state rinvenute cartelle cliniche abbandonate e alla portata di chiunque.

La documentazione riportante "dati sensibili" come diagnosi, radiografie, certificati medici ecc., è relativa a bambini malati di tubercolosi ospitati fino agli anni ottanta presso la struttura sanitaria che fungeva da colonia estiva. Struttura che, con il venir meno di questo tipo di iniziative a favore dei minori, è andata progressivamente in disuso fino alla sua definitiva dismissione oltre vent'anni fa.

Attivatosi immediatamente per accertare le eventuali violazioni della normativa sulla protezione dei dati personali, il Garante ha inviato sul posto il proprio nucleo ispettivo che ha assunto un ruolo di coordinamento degli interventi, già avviati, su indicazione della Procura presso il tribunale per i minorenni di Lecce, da parte delle autorità locali, allo scopo di verificare che recupero e conservazione delle cartelle cliniche avvenisse in modo idoneo così da evitare accessi non autorizzati ai dati personali.

2 febbraio 2004 - Medici di base, consenso e ricette: garanzie per i cittadini, senza burocrazia

Lettera del Garante al Ministro della Salute

Con riferimento ad alcune recenti polemiche relative all'applicazione del nuovo Codice in materia di protezione dei dati personali al settore sanitario, l'Autorità Garante ha inviato il 9 febbraio al Ministro della salute una nota di ringraziamento per la collaborazione prestata e per i commenti espressi dal Ministro in una lettera del gennaio scorso, riguardo al percorso di crescita di una cultura del rispetto dei diritti e delle libertà fondamentali delle persone interessate dai trattamenti di dati.

Nella lettera, il Garante ha anche indicato alcuni punti qualificanti della sua azione in favore di una applicazione delle norme che, mantenendo le più alte garanzie per i cittadini, non aggravino gli adempimenti burocratici.

Il Garante ha innanzitutto ricordato la collaborazione con il Governo ed il Parlamento, confermando il proprio impegno nella delicata fase di prima attuazione del Codice appena entrato in vigore per ricercare ogni soluzione utile per garantire diritti e libertà fondamentali nel rispetto del principio di semplificazione (art. 2 del Codice). Ha poi precisato che, con la collaborazione degli operatori sanitari, definirà a breve un modello semplificato di informativa agevolmente utilizzabile anche dai medici di base senza approcci burocratici (artt. 13, comma 3, e 78, comma 3).

L'Autorità ha inoltre anticipato che suggerirà agli operatori sanitari formule sintetiche e colloquiali per raccogliere gli eventuali consensi, anche in questo caso nell'ottica di prevedere garanzie efficaci anziché inutili soluzioni formalistiche, e tenendo presenti le varie situazioni nelle quali, dal 1° gennaio scorso, il consenso non è più necessario o può essere differito per assicurare la tempestività e l'efficacia della prestazione medica.

Il Garante ha confermato che è già a buon punto un proficuo confronto con la FNOMCeO (Federazione nazionale ordini dei medici chirurghi e odontoiatri) per permettere ai medici di base di non doversi privare dei dati dei propri assistiti che non dovessero entrare in contatto con essi entro il termine transitorio del 30 settembre 2004;

E' stato poi manifestato l'impegno a fornire a breve termine altri chiarimenti per porre fine agli allarmismi ingiustificati che si sono creati, specie per i medici di base, a proposito delle misure per rispettare la dignità e la riservatezza delle persone nelle sale d'attesa e riguardo alla notificazione dei trattamenti di dati al Garante.

Nella lettera viene anche anticipato che le misure da adottare per tutelare le persone nelle situazioni di promiscuità o in occasione di prestazioni sanitarie, in attuazione dell'art. 83 del Codice, interesseranno solo le strutture sanitarie e non le anticamere di singoli medici di base, i quali hanno un rapporto diverso e più personalizzato con i propri assistiti;

Per quanto riguarda la notificazione, il Garante ha precisato che tale adempimento, già notevolmente ridotto a pochissimi casi dal Codice, non interesserà l'intera categoria dei medici di base, riguardando esclusivamente alcuni particolari trattamenti di dati suscettibili di arrecare pregiudizio ai diritti e alle libertà delle persone e per i quali, in ossequio al chiaro dettato comunitario, è però irrinunciabile una trasparenza quale che sia l'operatore sanitario. Anche per questo aspetto l'Autorità interverrà con specifici chiarimenti ed eventuali semplificazioni (art. 37, comma 2). E' comunque già da escludere che si tratti di un adempimento gravoso: riguarda infatti solo una tantum l'intera attività svolta e non certo, caso per caso, ogni singolo rapporto con i pazienti.

Il Garante ha infine ringraziato il Ministero della ulteriore collaborazione che si svilupperà, entro il 1° gennaio 2005, sulla disciplina delle ricette mediche, fiduciosa del fatto che anche in questo caso si individueranno modalità attuative ragionevoli e praticabili per attuare le doverose scelte di garanzia più volte confermate dal Governo e dal Parlamento.

2 febbraio 2004 - No all'accanimento dei media sul caso della donna che rifiuta l'amputazione

In riferimento alla vicenda della donna che rifiuta l'operazione alla gamba, ritenuta dai medici necessaria per la salvarle la vita, il Garante per la protezione dei dati personali (Stefano Rodotà, Giuseppe Santaniello, Gaetano Rasi, Mauro Paissan), anche in considerazione delle esigenze di tutela della privacy espresse dalla famiglia, richiama gli organi di informazione al rispetto della dignità del malato, evitando forme di accanimento giornalistico.

In un momento particolarmente delicato per la donna, diffondere indirizzi e dati personali dell'interessata o insistere nella ricerca di particolari, finisce per ledere non solo la riservatezza ma la stessa libertà delle persone di autodeterminazione nel maturare in silenzio e tranquillità una difficile scelta personale.
(Comunicato del 3 febbraio 2004)

26 gennaio 2004 - Aziende sanitarie locali e privacy dei pazienti

Vanno adottate misure per migliorare il rapporto quotidiano con gli assistiti

Una azienda sanitaria romana è finita sotto la lente del Garante (Stefano Rodotà, Giuseppe Santaniello, Gaetano Rasi, Mauro Paissan) per non aver rispettato le norme sulla privacy.

In occasione del rilascio della tessera per l'esenzione dal pagamento del ticket la Asl avrebbe chiesto ad una malata anche copia del certificato medico che attesta la malattia dalla quale è affetta e che le dà diritto all'esenzione.

Nell'impossibilità di fare una fotocopia all'interno dell'ufficio pubblico, la paziente si era dovuta recare presso un vicino tabaccaio dove aveva trovato in attesa altri malati che seguivano la stessa trafila. Per avere la copia del certificato, dove era indicata la diagnosi di tumore, era stata dunque costretta ad esibirlo al tabaccaio del quartiere dove abita.

La donna aveva infatti denunciato il caso con una lettera ad un quotidiano nella quale raccontava quanto accaduto e lamentava la violazione dei più elementari diritti alla riservatezza.

Il Garante, venuto a conoscenza del fatto, ha immediatamente disposto accertamenti per verificare innanzitutto se vi sia stato un eccesso nella richiesta di dati personali all'interessata. Entro la fine di febbraio l'azienda sanitaria dovrà comunicare al Garante quali procedure utilizza per il rilascio dei documenti che consentono l'esenzione dal pagamento del ticket ed in base a quale norma verrebbe richiesta copia del certificato medico che attesta la patologia per la quale si chiede l'esenzione. L'azienda dovrà inoltre far sapere le misure che intende adottare, alla luce dell'entrata in vigore - il primo gennaio 2004 - del Codice sulla privacy, per assicurare il più possibile la dignità e la riservatezza delle persone che si recano presso i suoi uffici. Il nuovo Codice infatti prescrive una serie di accorgimenti che dovranno essere adottati dalle strutture sanitarie per migliorare il rapporto quotidiano con gli assistiti. Tra questi l'istituzione di appropriate distanze di cortesia, l'adozione di postazioni di lavoro riservate che non permettano, durante i colloqui, di far conoscere ai vicini informazioni sullo stato di salute, una maggiore tutela del segreto professionale al quale ora è tenuto anche il personale paramedico.

Nel caso l'azienda sanitaria non ottemperasse alle richieste del Garante rischia una sanzione amministrativa che va da quattro mila a 24 mila euro.

12 gennaio 2004 - Nel 2003 quasi triplicate le ispezioni del Garante

Il bilancio di un anno di attività

Nel settore privato aziende più grandi iniziano ad affrontare meglio la legge predisponendo anche "uffici privacy", avvalendosi magari di collaborazioni esterne, mentre aziende medio piccole trascurano di più la materia ed evidenziano un livello inferiore di adeguamento alla normativa e agli indirizzi del Garante. Nella pubblica amministrazione la cultura della privacy stenta ad affermarsi: processi di lavoro e gestione delle pratiche di ufficio poco rispettosi della legge sulla tutela dei dati personali e, in alcuni casi, assoluta noncuranza e superficialità nel trattamento dei dati.

Questo il quadro che emerge dalle 56 ispezioni che l'Ufficio del Garante, a cura del Dipartimento vigilanza e controllo, ha effettuato lo scorso anno nei confronti di pubbliche amministrazioni e privati. Complessivamente 30 in più rispetto al 2002.

L'incremento dell'attività ispettiva si è potuto realizzare anche grazie allo stretto rapporto di collaborazione con la Guardia di finanza stabilito con il protocollo siglato nell'ottobre 2002, che prevede uno stretto rapporto con il Comando Unità speciali del Corpo.

I controlli sono stati originati da segnalazioni di cittadini o di organi di stampa (48%), che hanno reso necessaria una verifica sul posto e da ricorsi (42%), dai quali sono emersi profili che meritavano accertamenti autonomi. Cicli di ispezioni e controlli incrociati, pari al 10% del totale, sono stati effettuati d'ufficio per verificare il rispetto della normativa in determinati settori.

Le ispezioni hanno riguardato nel 34% dei casi le modalità di acquisizione del consenso, soprattutto nell'ambito delle comunicazioni commerciali indesiderate via Internet e nel 26% il rispetto della normativa in materia di videosorveglianza.

In un ulteriore 26% dei casi l'ispezione ha accertato l'origine dei dati personali trattati mentre nel 12% ha verificato le misure di sicurezza. Gli interventi recenti sono stati effettuati su tutta la penisola, anche se in questa fase si sono concentrati nelle regioni settentrionali e centrali dove sono localizzate in prevalenza le aziende private controllate. Nel corso delle attività ispettive sono state accertate numerose violazioni amministrative e, nel 10% dei casi, si è proceduto ad inviare segnalazioni all'Autorità giudiziaria per violazioni costituenti reato quali: il trattamento illecito di dati personali, la mancata adozione delle misure di sicurezza, l'inottemperanza ai provvedimenti del Garante.

Alcune ispezioni hanno consentito inoltre di portare alla luce gravi inadempienze per l'accertamento delle quali sono state avviate complesse indagini di polizia giudiziaria ancora in corso.

L'esperienza ha evidenziato anche un buon rapporto istituzionale con i presidenti dei tribunali competenti per il territorio che, nei casi in cui occorreva una loro autorizzazione, hanno accolto tempestivamente con provvedimenti motivati le richieste dell'Autorità.

Per quanto riguarda il futuro, pubblica amministrazione, Internet, trattamento informatico dei dati saranno i settori sui quali maggiormente si concentrerà l'attività ispettiva del Garante Privacy. All'inizio dell'anno 2004 è stato rafforzato il rapporto di collaborazione con la Guardia di finanza, con l'obiettivo di incrementare ancora l'efficacia dell'attività di controllo dell'Autorità.

5 gennaio 2004 - Ricette in strada. Interviene il Garante

Proseguono gli accertamenti dell'Autorità Garante (Stefano Rodotà, Giuseppe Santaniello, Gaetano Rasi, Mauro Paissan) nei confronti di un'azienda sanitaria locale romana per verificare il rispetto di tutte le disposizioni in materia di misure minime di sicurezza per il trattamento di dati personali previste dal Codice sulla privacy (d. lg. n.196/2003). Il Garante dovrà accertare se l'episodio che si è verificato a fine dicembre, relativo a documentazione sanitaria (ricette, cartelle cliniche ancora leggibili, relativi ad un ingente numero di persone) rinvenuta nel corso di una ispezione nel cortile di una biblioteca comunale, liberamente accessibile al pubblico, costituisca un fatto imprevedibile, causato dall'incendio del magazzino in cui il materiale era raccolto, oppure non riveli una carenza da parte dell'azienda sanitaria nell'adozione delle misure minime di sicurezza.

I dati personali, in particolare quelli sensibili, devono essere custoditi in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito. La mancata adozione delle misure minime di sicurezza configura un illecito penale e può comportare l'ammenda da diecimila a cinquantamila euro o l'arresto sino a due anni. Dopo l'intervento del Garante l'azienda sanitaria ha rimosso la documentazione.

Il Garante, venuto a conoscenza della vicenda il 9 gennaio da fonti di stampa, ha disposto immediati accertamenti che hanno avuto luogo la mattina successiva. Il nucleo ispettivo dell'Autorità ha accertato che documenti sanitari, ricette di migliaia di cittadini, risalenti in prevalenza alla fine degli anni '80, in cui sono ancora leggibili nomi, cognomi, prescrizioni, date di emissione, giacevano incustoditi all'aperto in una zona di passaggio al pubblico dopo un incendio che il 23 dicembre scorso aveva interessato anche il prefabbricato in cui la Asl li conservava. La Asl sentita dagli ispettori del Garante sulla vicenda ha "giustificato" la permanenza della documentazione all'esterno con il ritardo nel reperimento di una ditta, a causa delle festività, dopo che la Croce rossa cui l'archivio "morto" era destinato, aveva fatto sapere che non era più interessata al recupero della carta perché inservibile.

Il Garante, in considerazione della gravità dell'accaduto, ha deciso dunque di continuare gli accertamenti sulle misure minime di sicurezza che l'Azienda normalmente adotta nel trattamento dei dati e definirà al più presto il relativo procedimento.

8 dicembre 2003 - Perizie medico-legali e privacy degli assicurati

L'accesso è consentito attraverso il medico designato dal cliente o dall'assicurazione

Le informazioni personali comprese nelle valutazioni e negli altri elementi di giudizio riportati nelle perizie medico-legali delle compagnie di assicurazione rientrano nella sfera dei dati personali e vanno pertanto comunicate, quando l'interessato le richiede e quando riguardano la salute, per il tramite di un medico designato da lui stesso o dalla compagnia assicuratrice titolare del trattamento.

Il principio è stato ribadito dall'Autorità Garante (Stefano Rodotà, Giuseppe Santaniello, Gaetano Rasi e Mauro Paissan) nella decisione sul ricorso di un cittadino che, a seguito di un sinistro di cui era rimasto vittima, si era rivolto alla società assicuratrice della controparte per avere conferma dell'esistenza di dati personali che lo riguardavano.

I ripetuti solleciti svolti dall'interessato non avevano però prodotto alcun risultato spingendo quindi il ricorrente a rivolgersi all'Autorità. In particolare, nel ricorso presentato al Garante, l'interessato specificava di aver chiesto invano, per il tramite del suo medico di fiducia, la comunicazione dei dati personali riguardanti il suo stato di salute contenuti nella perizia medico-legale, redatta sulla base dei documenti sanitari e degli altri elementi emersi nel corso delle visite mediche alle quali si era sottoposto dopo l'incidente.

La compagnia, invitata dal Garante ad aderire spontaneamente alle richieste, riconosceva a quel punto di essere in possesso dei dati personali del richiedente e provvedeva a trasmettere la perizia medico-legale redatta dal fiduciario della società al medico di fiducia designato dal ricorrente.

24 novembre 2003 - Accesso ai dati personali da parte dei lavoratori

Garanzie e limiti nell'uso delle norme sulla privacy

Il diritto di accesso regolato dalla normativa sulla privacy consente al lavoratore di accedere a tutti i dati che lo riguardano detenuti dal proprio datore di lavoro, ma non può essere esercitato per conoscere notizie di carattere contrattuale o professionale (quali, ad esempio, gli accordi collettivi nazionali od aziendali), se non strettamente e direttamente riferite all'interessato.

Il principio è stato affermato dall'Autorità (Stefano Rodotà, Giuseppe Santaniello, Gaetano Rasi e Mauro Paissan) chiamata a rispondere sul ricorso di un dipendente di una società di servizi che reclamava di non aver ricevuto idoneo riscontro a varie istanze, formulate in base alla legge n. 675/1996, con le quali lamentava il fatto di non essere stato adeguatamente informato delle mansioni da svolgere in relazione al proprio profilo professionale da parte del responsabile della struttura di appartenenza, malgrado esistesse un documento "ufficiale" aziendale che lo riguardava.

In particolare, il dipendente nel ricorso al Garante chiedeva di accedere ai dati personali detenuti dal suo datore di lavoro sia nel loro complesso, sia in riferimento alla comunicazione "in forma scritta ed ufficiale" di dati relativi ai compiti e alle mansioni riguardanti il suo profilo professionale di appartenenza. Chiedeva inoltre che gli venissero comunicati "dati, notizie e quant'altro (...)" di propria "pertinenza" in possesso dell'azienda.

La società, invitata dal Garante ad aderire alle richieste, forniva ulteriori informazioni, integrative rispetto a quelle già comunicate all'interessato, in merito all'individuazione delle mansioni cui il dipendente era adibito, inviando anche copia dei documenti aziendali precedentemente elaborati per descrivere le attività relative al profilo professionale di appartenenza del ricorrente.

La società precisava, infine, di non possedere altri dati riferiti all'interessato connessi al suo profilo professionale.

Nel decidere il ricorso, il Garante ha stabilito che non rientra nell'ambito di applicazione della legge 675/1996, la richiesta di conoscere notizie di carattere contrattuale o professionale che non hanno natura di dati personali in qualche modo riferibili a persone identificate o identificabili come, ad esempio, gli accordi collettivi nazionali od aziendali.

In considerazione del riscontro, seppure tardivo, dato alle richieste dell'interessato da parte della società, a quest'ultima sono state addebitate in misura forfetaria solo parte delle spese del procedimento.

27 ottobre 2003 - Malattie professionali: lecite le segnalazioni dei medici all'Inail

I medici che diagnosticano ai loro pazienti malattie che possono essere state provocate da determinate attività lavorative potenzialmente nocive possono trasmettere direttamente all'Inail la denuncia della diagnosi.

Lo ha confermato il Garante nella risposta al quesito di un ufficio giuridico che chiedeva di verificare la legittimità, rispetto alla normativa sulla privacy, della trasmissione direttamente da parte dei medici all'Istituto assicuratore delle denunce di alcune malattie collegate alle attività lavorative dei loro pazienti.

Generalmente la denuncia dell'insorgenza di malattie professionali, corredata del certificato medico contenente il domicilio dell'ammalato, il luogo in cui è ricoverato e una relazione sulla sintomatologia accusata dal paziente e una su quella rilevata dal medico certificatore, viene trasmessa dal datore di lavoro all'Istituto assicuratore, entro i cinque giorni successivi a quello nel quale il prestatore d'opera ha fatto denuncia al datore di lavoro della manifestazione della malattia (art. 53 del d. P.R. n. 11124/1965), con l'obbligo per il medico, qualora l'Inail le richieda, di fornire tutte le notizie ritenute necessarie all'espletamento della causa.

Rispetto ad alcune malattie professionali elencate in un decreto vige tuttavia comunque nell'attuale ordinamento giuridico l'obbligo - per il medico che venga a conoscenza nell'esercizio della sua attività di determinate malattie professionali - di denuncia, oltre che all'azienda sanitaria locale, anche alla sede dell'Istituto assicuratore competente per territorio (art. 139 del d.P.R. n. 1124/1965 e art. 10 del decreto legislativo n.38/2000). Va ricordato, a tale proposito, che la pertinente normativa stabilisce che l'elenco delle malattie professionali, contenga anche una lista di malattie di probabile e di possibile origine lavorativa da tenere sotto osservazione ai fini dell'eventuale revisione dell'elenco.

Per quanto concerne, poi, le disposizioni in materia di protezione dei dati personali, l'art. 112 del nuovo Codice, in vigore dal prossimo 1° gennaio 2004, considera di rilevante interesse pubblico i trattamenti di dati finalizzati all'attuazione della disciplina in materia di igiene e sicurezza del lavoro.

Pertanto, non ravvisandosi un contrasto con il quadro normativo vigente, l'Autorità ha ribadito che non sussiste il divieto per i medici a trasmettere direttamente all'Inail la segnalazione delle predette malattie professionali potenzialmente nocive, corredate da un'anamnesi lavorativa e dai rischi e dalle sostanze alle quali il lavoratore sia, o sia stato, esposto nello svolgimento della sua prestazione professionale, purché ciò avvenga nel rispetto delle finalità prescritte dalle specifiche disposizioni in materia di assicurazioni contro gli infortuni sul lavoro e le malattie professionali quali quelle previste dal principio di pertinenza (art. 9, legge 675/1996) in merito agli scopi per i quali i dati vengono raccolti.

13 ottobre 2003 - Incontro Garante-Fnomceo

Iniziative per venire incontro alle esigenze della categoria in vista delle nuove norme sulla privacy

Si è svolto il previsto incontro tra l'Autorità Garante e la Federazione Nazionale dei medici chirurghi e degli odontoiatri (FNOMCEO). All'incontro, presieduto dal presidente dell'Autorità, Stefano Rodotà, e dal presidente della Federazione, Giuseppe Del Barone, hanno partecipato, per l'Autorità, il Segretario generale Giovanni Buttarelli e, per la FNOMCEO, il presidente dell'Ordine dei medici di Savona, Renato Giusto, il presidente dell'Ordine dei medici di Cuneo, Renato Palanca, il presidente dell'Ordine dei medici di Bari, Francesco Lo Surdo, il Presidente della Commissione odontoiatrica di Avellino, Raffaele Iandolo, e la dott.ssa Rossella Procino.

L'incontro ha avuto lo scopo di sviluppare le già concordate forme di collaborazione per graduare e pianificare l'applicazione del nuovo Codice in materia di protezione dei dati personali. In particolare, sono state nuovamente esaminate le modalità per la prima attuazione delle disposizioni sul consenso, a partire dal 30 settembre 2004, e in materia di ricette mediche, entro il primo gennaio 2005.

Sono stati quindi individuati vari possibili accorgimenti per venire incontro ad esigenze pratiche della categoria e, al tempo stesso, per introdurre ulteriori garanzie previste dal Codice.

In particolare, in relazione alla nuova disciplina della raccolta del consenso, verrà approfondita nei prossimi giorni la richiesta della categoria, e più specificamente dei medici di famiglia, di poter conservare temporaneamente, senza utilizzarli in concreto, i dati relativi a propri assistiti che gli stessi medici già detengono in base a dettami di passate convenzioni, in attesa del primo contatto con gli interessati o nell'eventualità che tale contatto non si verifichi entro la predetta data del 30 settembre.

Seguiranno a breve, come programmato e sulla base dell'apporto di un gruppo di lavoro, altri incontri per mettere a punto nuove iniziative, anche in collaborazione con assessori regionali.
(COMUNICATO DEL 16 OTTOBRE 2003)

6 ottobre 2003 - Polizze assicurative e privacy

L'erede può conoscere i dati del defunto, ma non quelli dei beneficiari di una polizza

Il diritto di accesso ai dati di un defunto non riguarda informazioni relative a terzi, come ad esempio i beneficiari di polizze assicurative.

Questa la sostanza del provvedimento emesso dall'Autorità dopo aver esaminato il ricorso dell'erede legittimo di una donna che, poco prima di morire, aveva stipulato con una società di assicurazioni una polizza a favore di un terzo le cui generalità non erano note al ricorrente. Il Garante, infatti, pur riconoscendo all'erede legittimo il diritto ad accedere a tutte le informazioni personali che riguardano la defunta, non ha consentito alla società assicuratrice di comunicare il nome del beneficiario della polizza.

La vicenda prende avvio da un'istanza avanzata dall'erede alla società di assicurazioni allo scopo di ricevere informazioni e notizie riguardanti la stipula della polizza di assicurazione sottoscritta dalla defunta e volta ad ottenere anche copia della stessa polizza.

Davanti al rifiuto della società non solo a fornire la documentazione, ma anche a dare all'interessato informazioni verbali al riguardo, l'erede si rivolgeva al Garante chiedendo che gli fosse riconosciuto il diritto di ricevere in forma intelligibile i dati riguardanti la polizza, l'origine del contratto di assicurazione, l'esistenza di dati contenuti nella polizza, ribadendo anche nel ricorso la richiesta di voler ricevere dalla controparte copia della polizza, eventualmente corredata da notizie relative ad eventi verificatisi successivamente alla data di stipula.

La società resistente, invitata dall'Autorità ad aderire alle richieste, ribadiva però il proprio rifiuto sostenendo che, accogliendo le richieste dell'erede, si poteva integrare l'ipotesi di illecita comunicazione di dati personali perché di fatto sarebbero state rese note le generalità del beneficiario, mentre il disposto dell'art. 13, della legge n. 675/1996, andrebbe interpretato proprio al fine di tutelare l'interesse della persona deceduta a non divulgare i dati del beneficiario della polizza da lei sottoscritta.

Nel provvedimento il Garante ha riconosciuto legittima la richiesta del ricorrente di accedere ai dati personali riconducibili alla defunta, benché impropriamente formulata nella parte in cui si chiedeva l'accesso ad interi documenti detenuti dalla società di assicurazioni.

La messa a disposizione dell'intera documentazione da parte del titolare del trattamento, in copia o in visione, può infatti essere permessa - ha ribadito l'Autorità - solo qualora sussistano reali, oggettive difficoltà di estrapolazione dei dati richiesti all'interno di documenti, e comunque avendo cura di oscurare i dati personali eventualmente riferiti a terzi.

In tal senso, alla società resistente è stato intimato di estrarre dagli atti e dai documenti da essa detenuti, comprese pertanto le eventuali polizze sottoscritte, tutte le informazioni personali relative alla defunta, comunicandole in modo intelligibile

all'erede legittimo, avendo però cura di escludere tutte le informazioni non direttamente riferite alla signora scomparsa e, quindi, nello specifico, non comunicando i dati personali relativi al beneficiario della polizza.

22 settembre 2003 - No degli esperti UE ai test genetici sui lavoratori

Inaccettabili sul piano etico, discriminatori sul piano sociale

Niente *test* genetici sui lavoratori né prima né dopo l'assunzione. Non sono necessari per adempiere agli obblighi del datore di lavoro in materia sanitaria o per la valutazione attitudinale dei dipendenti e la selezione degli aspiranti lavoratori. Si può ricorrere allo *screening* genetico solo in casi del tutto eccezionali, espressamente previsti e regolati dalla legge, a fini di tutela della salute, e comunque con il consenso informato dei lavoratori. Allo stato attuale delle conoscenze scientifiche l'affidabilità e il valore predittivo dei test sono ancora controversi.

Queste, in sintesi, le conclusioni formulate nel parere che il Gruppo Europeo sull'Etica nelle Scienze e nelle Nuove Tecnologie, costituito da esperti indipendenti dei 15 Paesi membri UE (l'Italia è rappresentata da Stefano Rodotà), ha pubblicato di recente in merito agli "Aspetti etici dei *test* genetici sul luogo di lavoro" (il documento è disponibile

all'indirizzo <http://europa.eu.int/...> ).

Il Gruppo, che riferisce direttamente al presidente della Commissione Europea, è giunto alla formulazione di questo parere all'esito di un lungo processo di analisi avviato con una tavola rotonda a Bruxelles nel 2000 ed articolatosi in numerosi incontri nei primi mesi del 2003.

Il parere riguarda lo "*screening* genetico", ossia i *test* genetici condotti per individuare l'eventuale presenza di (o suscettibilità a) alterazioni nel patrimonio genetico di una persona. Diverso è invece il caso del "monitoraggio genetico", ossia l'esecuzione di indagini genetiche a intervalli regolari per verificare se le condizioni dell'ambiente di lavoro, in sé potenzialmente nocive, abbiano portato ad alterazioni del patrimonio genetico dei dipendenti. Il Gruppo tiene a sottolineare, tuttavia, che le conclusioni complessive ed il contesto di riferimento del parere restano validi anche per il monitoraggio genetico.

E' evidente l'interesse che i risultati di simili *test* rivestono per i datori di lavoro, nonché per le compagnie di assicurazione chiamate a stipulare, ad esempio, polizze-vita con i dipendenti di una specifica azienda. Pertanto, il Gruppo ha ritenuto di dover chiarire i presupposti scientifici, giuridici ed etici che fanno attualmente da sfondo alla valutazione di questo tema.

Sul piano scientifico, la **validità** dei *test* genetici è ancora molto controversa. La loro **affidabilità** è inficiata dalla presenza di numerosi falsi negativi e falsi positivi, ed il **valore predittivo** è limitato – soprattutto nel caso delle patologie poligeniche, ossia dovute all'interazione di più alterazioni genetiche. In queste circostanze è praticamente impossibile prevedere se la patologia insorgerà, ed eventualmente quando o con quale gravità. Il Gruppo mette in guardia contro i rischi del "determinismo genetico", e sottolinea gli effetti dovuti ai fattori ambientali ed allo stile di vita.

Sul piano giuridico, **a livello internazionale non esistono norme dedicate espressamente al tema dei test genetici sul luogo di lavoro**; in particolare, non ci sono disposizioni che disciplinino le modalità di raccolta e trattamento dei dati genetici. Peraltro, in molti Paesi UE **esistono norme nazionali** che, ad esempio, vietano la discriminazione basata sui risultati di *test* genetici predittivi, oppure vietano del tutto l'esecuzione di *test* genetici sul luogo di lavoro (ai fini dell'assunzione o durante il rapporto di lavoro). Va ricordato, a questo proposito, che in Italia il trattamento di dati genetici è consentito solo con l'autorizzazione del Garante alle condizioni indicate in tale autorizzazione. Inoltre, è allo studio della Commissione una proposta di Direttiva che intende fornire un quadro armonizzato a livello europeo per tutelare i dati personali sul luogo di lavoro, secondo i principi della direttiva "madre" (95/46/CE).

Sul piano etico, il Gruppo distingue fra **esecuzione dei test** ed **utilizzo dei relativi risultati**. Rispetto all'esecuzione di *test* di *screening* esiste l'esigenza di **bilanciare l'autonomia del lavoratore** (o del candidato all'impiego) **con gli obblighi del datore di lavoro concernenti la tutela della propria forza-lavoro e di terzi**. Il datore di lavoro è tenuto al rispetto di tali obblighi (anche per garantire la sicurezza dell'ambiente di lavoro), ma per valutare l'efficienza del lavoratore sono sufficienti normalmente gli strumenti tradizionali (*curriculum vitae*, colloquio, *test* attitudinali, referenze, visita medica *standard*), senza contare che in genere è previsto un periodo di prova precedente l'assunzione definitiva, circostanza che costituisce un'ulteriore salvaguardia per il datore di lavoro. Inoltre, la ridotta predittività dei *test* genetici e la loro scarsa affidabilità non permettono di considerare equa una decisione importante - come quella di assumere o promuovere un dipendente - che si basi sui risultati di tali *test*. Inoltre, **l'autonomia** di cui parla il Gruppo **si fonda in primo luogo sul consenso veramente informato del lavoratore**, ed il Gruppo non manca di rilevare che in questo contesto la **validità del consenso è dubbia** essendo il lavoratore la parte "debole" del rapporto.

L'utilizzazione delle informazioni ricavate dai *test* pone, secondo gli esperti UE, due ordini di problemi: la necessità di mantenere riservate tali informazioni e di garantire il diritto del dipendente di non essere informato dei risultati in questione, da un lato, e, d'altro canto, il rischio che tali risultati siano utilizzati per finalità discriminatorie – ad esempio, impedendo la promozione e quindi compromettendo la carriera di uno specifico lavoratore.

Ecco, dunque, i punti salienti del parere formulato dai Garanti:

- a) I lavoratori ed i candidati all'impiego devono considerare normale l'esecuzione di una visita medica per valutare l'attitudine ad una determinata attività; tuttavia, **la visita medica non deve costituire un criterio di selezione**, e deve essere effettuata dopo che la fase di selezione si è conclusa.
- b) Lo *screening* genetico è un esame medico e riguarda la potenziale evoluzione dello stato di salute di una persona; **nel contesto lavorativo, si deve tenere conto soltanto dello stato di salute corrente del lavoratore.**

- c) Il Gruppo ritiene inaccettabile sul piano etico ricorrere allo *screening* genetico nell'ambito di una visita medica, o comunicare i risultati di *test* genetici pregressi. **I test genetici non sono necessari per garantire il rispetto degli obblighi e dei diritti legittimi del datore di lavoro in materia sanitaria, o per la valutazione attitudinale; pertanto, in linea di principio, i datori di lavoro non dovrebbero ricorrere a test genetici di screening né chiedere ai lavoratori di sottoporsi a test del genere.**
- d) **Il ricorso ai test genetici di screening deve costituire un'eccezione**, al fine di garantire la tutela della salute dei lavoratori o di terzi, e deve essere effettivamente **necessario**, deve fondarsi sulla **provata validità scientifica** del *test*, deve essere **proporzionato** alle finalità da raggiungere e non deve comportare alcuna **discriminazione** per i lavoratori coinvolti.
- e) **I casi eccezionali** nei quali è ammissibile effettuare *test* genetici di *screening* sul luogo di lavoro devono essere **specificati espressamente per legge**, eventualmente prevedendo il coinvolgimento di organismi sindacali e di enti indipendenti di controllo.
- f) E' indispensabile il **consenso informato** del lavoratore o del candidato all'impiego, che deve avere la possibilità di ricorrere ad un consulente legale indipendente.
- g) **I dati genetici devono rimanere riservati** come ogni altro dato sanitario; ogni comunicazione a terzi, compreso il datore di lavoro, è vietata senza il consenso dell'interessato. In particolare, **i risultati di test di screening o di monitoraggio effettuati sul luogo di lavoro non devono essere comunicati a fini assicurativi.**

15 settembre 2003 - Cartelle cliniche e privacy

Si può avere accesso ai dati sulla salute solo se il diritto che si intende far valere è di "pari rango" rispetto a quello del malato

Cartelle cliniche, fascicoli personali e, in generale, documenti che contengono informazioni sullo stato di salute detenuti da un'amministrazione pubblica, possono essere accessibili da persone diverse dal "malato" solo se il diritto che si intende far valere in giudizio è di "pari rango", ossia dello stesso livello, di quello della persona cui si riferiscono i dati. La comunicazione dei dati è giustificata e legittima solo se il diritto del richiedente rientra nella categoria dei diritti della personalità o è compreso tra altri diritti o libertà fondamentali e inviolabili (artt. 71, 92 e 60 del Codice in materia di protezione dei dati personali). In ogni altra situazione prevale la tutela della riservatezza, della dignità e degli altri diritti fondamentali del malato.

Questi i principi guida contenuti nel provvedimento generale, adottato a seguito di numerosi quesiti e segnalazioni, con il quale l'Autorità Garante indica le regole e i limiti per prendere visione ed estrarre copia di atti e documenti che contengono informazioni sanitarie da parte di persone diverse dal soggetto cui i dati si riferiscono. I quesiti e le segnalazioni poste al Garante riguardavano, in particolare, le richieste di accesso rivolte ad amministrazioni pubbliche (per le quali l'Autorità ha ribadito l'applicabilità delle norme sulla trasparenza amministrativa), l'accesso alle cartelle cliniche detenute presso le strutture sanitarie e le richieste avanzate dai difensori ai sensi della normativa vigente.

Le informazioni sullo stato di salute e la vita sessuale - ha precisato nella sua pronuncia l'Autorità - sono oggetto, per la loro particolare delicatezza, di una speciale protezione. Il trattamento di queste informazioni, infatti, è vietato a livello internazionale e comunitario, ad eccezione di alcuni casi in cui è permesso per perseguire importanti finalità e con specifiche ed elevate garanzie. Lo stesso impianto, già recepito dalla legge sulla privacy, è stato confermato e rafforzato nel recente "Codice in materia di protezione dei dati personali" (decreto legislativo n. 196 del 30.6.2003), che entrerà in vigore il 1 gennaio 2004.

Per la valutazione del "pari rango", l'amministrazione o la struttura privata, alle quali venga richiesto l'accesso ai dati, devono far riferimento al diritto che la persona intende difendere in giudizio sulla base del materiale documentale che chiede di conoscere.

Ma occorre valutare, anche, che tutti i dati richiesti siano effettivamente "necessari" all'esercizio o alla difesa di diritti equivalenti a quello di riservatezza e, nel caso, accogliere parzialmente la richiesta e comunicare solo le informazioni necessarie.

La valutazione dei diritti di "pari rango" si applica anche nell'ipotesi in cui la richiesta di accesso o di comunicazione dei dati sanitari sia avanzata da un difensore, nell'ambito di investigazioni difensive, o nella comunicazione da parte di un soggetto privato (ad esempio una casa di cura) di singoli dati personali sulla salute o la vita sessuale.

21 luglio 2003 - Adozioni: una banca dati sui minori solo con precise garanzie

Il Garante chiede maggiori tutele per famiglie e bambini dichiarati adottabili

Dati personali e sanitari, informazioni su condizioni socio-familiari, livelli di reddito e culturali relativi a minori adottabili, a coniugi e a persone singole che aspirano all'adozione sia nazionale, sia internazionale confluiranno in una unica banca dati che si sta costituendo presso il Dipartimento per la Giustizia minorile con lo scopo di migliorare le procedure di adozione ed accelerarne i tempi. Proprio in considerazione della rilevanza sociale di questo archivio, e della delicatezza delle informazioni raccolte, l'Autorità garante, in un parere preliminare reso al Ministero della giustizia che sta predisponendo un regolamento, chiede che siano introdotte maggiori garanzie e misure di sicurezza più adeguate. Nella banca dati degli adottabili, istituita nel 2001 dalla legge n. 149, confluiranno infatti automaticamente, tramite i registri informatizzati degli uffici della giurisdizione minorile (tribunali, procure, giudici tutelari ecc.) delicate informazioni riferite ai soggetti che concorrono alla procedura di adozione. L'accesso alla banca dati sarà probabilmente riservato ai magistrati del settore minorile, al personale giudiziario autorizzato e, limitatamente ai loro dati personali, agli interessati.

Nel parere, l'Autorità ha sottolineato la necessità di introdurre alcune modifiche per rendere maggiormente conforme il regolamento ai principi in materia di privacy. Ha chiesto anzitutto che vengano specificati nel dettaglio i soggetti che possono trattare i dati personali necessari per il funzionamento dell'archivio informatico, chiarendo quali sono quelli in concreto autorizzati a inserire o modificare i dati. Particolari garanzie dovranno essere previste per le informazioni di provenienza

extragiudiziaria, evitando riferimenti a generiche informazioni utili al procedimento (alla banca dei minori adottabili confluiranno, peraltro, anche dati forniti dalle regioni). Inoltre, l'identificazione e la "tracciabilità" dei soggetti che hanno accesso alla banca (consentite per seguire le operazioni di implementazione dell'archivio o le consultazioni, per garantire esigenze di sicurezza del sistema o per fini statistici) non dovrebbero essere realizzate attribuendo ai soggetti un codice di identificazione. La disciplina di tale modalità infatti, oltre ad essere oggetto del Codice sulla privacy n. 196/2003 di recente approvazione, richiede specifiche garanzie ed una attribuzione selettiva anche secondo la precedente normativa nazionale e comunitaria. I dati da inserire nella banca dati infine, vanno indicati puntualmente senza margini di discrezionalità e, per quelli di carattere sensibile, è stata sottolineata l'opportunità di prevedere più livelli di accesso ai dati per fasce di utenti differenziate (magistrati, cancellieri etc.), nonché di specificare anche le operazioni che con tali dati possono essere eseguite all'interno della banca dati.

2 giugno 2003 - Pensioni e trasparenza

Chiarezza nelle informazioni comunicate al pensionato

Al pensionato che chiede di conoscere i dati personali relativi alla propria pensione devono essere comunicate informazioni chiare e comprensibili. L'ente previdenziale deve fornire un riscontro completo e rapido, estrapolando i dati e comunicandoli al richiedente gratuitamente.

Il principio è stato ribadito dall'Autorità Garante alla quale si era rivolto, con un ricorso, un pensionato che lamentava la difficile comprensione e la parzialità delle informazioni contenute nella documentazione ricevuta dall'ente previdenziale. All'interessato erano state infatti consegnate le stampe relative ai ratei della pensione erogata, desunte direttamente dal programma informatico in uso nell'ufficio, e prive di informazioni aggiuntive o codici interpretativi. Peraltro, il pensionato aveva ricevuto ulteriori indicazioni su trattenute operate, modalità di pagamento e uffici pagatori solo dopo l'intervento del Garante. L'ente riteneva, comunque, di aver soddisfatto in questo modo le richieste del pensionato comunicando quanto in suo possesso e dichiarandosi non in grado di fornire ulteriori informazioni, poiché altra corrispondenza era depositata nel fascicolo presso il tribunale ove pendeva una controversia giudiziaria tra le due parti.

La richiesta del ricorrente - ha affermato l'Autorità - era legittima. Il diritto di avere accesso al complesso dei dati personali riconosciuto dalla legge sulla privacy ha caratteristiche peculiari e non deve essere confuso con il diverso diritto di accesso ai documenti amministrativi (legge 241/1990). Alla richiesta presentata ai sensi dell'art 13 della legge 675, il titolare del trattamento (cioè chi usa e conserva i dati) deve fornire un riscontro completo e tempestivo, a prescindere dal fatto che alcune informazioni siano eventualmente già nella disponibilità del richiedente. Le informazioni, inoltre, devono essere estratte dalla banca dati e comunicate gratuitamente; l'ente è tenuto poi a rendere agevole la loro comprensione riportandole su supporto cartaceo o informatico e, se richiesto, trasmesse per via telematica. Solo nel caso in cui vi siano reali difficoltà obiettive ad estrarre i dati, il titolare può far visionare gli atti o consegnarne copia, avendo cura di oscurare informazioni riferite a terzi.

Nel caso esaminato, invece, non risultava possibile decifrare (in particolare dalle stampe relative ai pagamenti della pensione) le informazioni personali a causa della mancanza di criteri, informazioni aggiuntive o codici interpretativi.

L'Autorità ha, quindi, ordinato all'ente previdenziale di comunicare al pensionato in modo intelligibile, entro un termine stabilito, il complesso dei dati personali in suo possesso, e se disponibili, anche quelli presenti nel fascicolo processuale.

14 aprile 2003 - Sanità: maggiore privacy per l'assistenza a domicilio

Il diario clinico del paziente non va inviato alla Asl

Presa di posizione del Garante, a seguito della segnalazione di un cittadino, nei confronti di una Asl che, giustificando il proprio comportamento con finalità di controllo dell'erogazione dei servizi e di elaborazione statistica, richiedeva ai propri medici di base l'invio, trimestrale, dei diari tenuti presso il domicilio dei pazienti beneficiari del servizio di assistenza domiciliare programmata (ADP).

La disciplina in materia, recentemente regolata dal d.P.R. n. 270/2000, art. 1, comma 1, prevede infatti, la tenuta, al domicilio del paziente, di un'apposita scheda degli accessi fornita dalla Azienda sanitaria, sulla quale sono annotate le eventuali considerazioni cliniche, la terapia, gli accertamenti diagnostici, le richieste di visite specialistiche, le prestazioni aggiuntive, le indicazioni del consulente specialista e quant'altro ritenuto utile e opportuno. In detto decreto, però, nessuna disposizione prevede l'inoltro di tali schede alle Asl competenti, neanche ai fini di controllo dell'erogazione dei servizi di assistenza domiciliare.

L'Autorità ha pertanto ritenuto illegittima la richiesta dell'Azienda sanitaria di una sistematica comunicazione di tali dati sensibili come quelli relativi allo stato di salute. A seguito di tale intervento, la Asl si è impegnata a rendere "immediatamente applicabile" l'indicazione fornita dal Garante di far trasmettere i soli fogli (e non le schede) che il medico firma ogni volta che effettua una visita domiciliare, senza alcuna indicazione della patologia riscontrata.

31 marzo 2003 - La cartella clinica deve essere leggibile

Il Garante chiede maggiori tutele per i pazienti

Se la cartella clinica è illeggibile per la grafia di chi l'ha redatta, deve essere trascritta in modo che le informazioni in essa contenute risultino chiare per il malato. La leggibilità delle informazioni è la prima condizione per la loro piena comprensione.

Lo ha precisato l'Autorità Garante accogliendo il ricorso di un paziente che lamentava un riscontro inadeguato da parte dell'azienda ospedaliera cui si era rivolto chiedendo la comunicazione in forma intelligibile dei dati personali contenuti nella sua cartella clinica. In risposta aveva ricevuto copia della cartella che, però, a suo parere, risultava illeggibile per la pessima

grafia degli autori e quindi incomprensibile. Nel ricorso il malato chiedeva che le spese del procedimento fossero attribuite all'azienda ospedaliera.

Nel provvedimento l'Autorità ha sottolineato la specifica tutela che la legge sulla privacy garantisce alle persone al momento dell'accesso ai propri dati personali, rispetto al diverso diritto di accesso agli atti e documenti amministrativi disciplinato dalla legge 241/1990. L'art 13 della legge 675/1996 prevede, infatti, che i dati personali devono essere estratti e comunicati all'interessato in forma intelligibile ed il principio viene ulteriormente specificato nel d.P.R. 501/1998, quando in riferimento ad alcune modalità di riscontro al diritto di accesso, si afferma che la comprensione dei dati deve essere agevole e obbliga il titolare del trattamento ad adottare opportune misure per agevolare l'accesso ai dati da parte degli interessati. Anche nel caso in cui l'estrazione e la trasposizione dei dati su un supporto cartaceo o informatico dovesse risultare particolarmente difficoltosa, la richiesta di accesso ai dati personali, formulata ai sensi della legge sulla privacy, può essere soddisfatta dall'esibizione o dalla consegna in copia di un documento, ma la leggibilità delle informazioni è la prima condizione, necessaria anche se non sufficiente, per la loro comprensibilità.

Riconosciuta, quindi, la legittimità delle richieste del ricorrente, il Garante ha ordinato all'azienda ospedaliera di rilasciare, entro un termine stabilito, una trascrizione dattiloscritta o comunque comprensibile delle informazioni contenute nella cartella clinica e di comunicarle all'interessato, come prescrive la legge, tramite il medico di fiducia o designato dalla Asl. All'Azienda sono state inoltre imputate le spese del procedimento, stabilite in 250 euro, che dovranno essere versate direttamente a favore del ricorrente.

10 febbraio 2003 - Marittimo sieropositivo licenziato. Il Garante avvia accertamenti (comunicato del 7 febbraio)

L'Autorità Garante ha deciso di avviare una procedura di accertamento per valutare se siano state violate le disposizioni legislative che tutelano la riservatezza e la dignità umana riguardo al caso, riportato oggi dalla stampa, del marittimo affetto da sindrome da Hiv licenziato dall'azienda per la quale lavorava.

9 dicembre 2002 - Perizie mediche: sanzionata un'assicurazione

Contestata una sanzione amministrativa di oltre cinquecento euro ad una società di assicurazioni per aver violato le disposizioni stabilite dalla legge sulla privacy in caso di comunicazioni di dati sullo stato di salute. L'assicurazione è stata "multata" per aver consegnato direttamente ad un suo assistito, che ne aveva fatto richiesta, copia di una perizia medica senza rispettare la disposizione che prevede la comunicazione di dati sanitari solo tramite il medico di fiducia dell'interessato o designato da chi detiene ed usa i dati, cioè da quello che la legge chiama "il titolare del trattamento".

L'assicurato era ricorso all'Autorità dopo aver chiesto invano alla società l'accesso ai suoi dati personali contenuti nella perizia medico legale redatta dal medico di fiducia dell'assicurazione. Solo dopo l'intervento del Garante, la società, pur fornendo giustificazioni sul suo comportamento omissivo, ritenute in parte fondate dal Garante, si dichiarava disponibile a soddisfare le richieste del suo assicurato e gli inviava copia della relazione di accertamento medico legale, con la descrizione delle circostanze del fatto, l'elenco della documentazione sanitaria, il referto di visita medica ed parere medico legale. Tuttavia la comunicazione di questi ultimi dati veniva effettuata dalla società direttamente all'interessato e non invece, secondo le modalità previste dalla legge 675/96, avvalendosi di un medico designato.

Dopo aver, quindi, verificato i presupposti per l'applicazione della sanzione amministrativa prevista per questo tipo di violazione, l'Autorità ha quindi provveduto a contestare la violazione amministrativa stabilita in 516,46 euro.

L'assicurazione potrà provvedere al pagamento in misura minima pari a 516, 456 euro, entro 60 giorni dalla contestazione della notifica o a far pervenire entro i primi trenta giorni memorie difensive.

14 ottobre 2002 - Ingunzione di pagamento per una Asl

Confermata la sanzione amministrativa pari a 1.032 euro contestata a suo tempo dall'Autorità garante ad un'azienda sanitaria locale.

I fatti iniziano due anni fa quando la Asl convocava "a visita medico-legale per l'accertamento dello stato invalidante e dell'handicap" un ragazzo minorenni, utilizzando un foglio piegato, privo di busta - il cui contenuto poteva dunque facilmente essere letto da chiunque - che riportava non solo le generalità dell'interessato, ma anche l'oggetto della convocazione, informazioni personali, cioè, attinenti al suo stato di salute e soggetti ad una speciale tutela in quanto dati sensibili.

I genitori si appellavano al Garante, segnalando la circostanza e accusando la struttura sanitaria di aver violato la riservatezza dei dati personali del minore. La Asl, sollecitata più volte dall'Autorità a fornire chiarimenti sull'accaduto, non dava tuttavia alcuna risposta.

In ragione di tale comportamento, l'Autorità adottava nell'aprile scorso il provvedimento con il quale contestava alla Asl la violazione delle disposizioni della legge 675/96 riguardanti la mancata risposta alla richiesta di informazioni o esibizioni di documenti (art. 39, comma 1) e applicava una sanzione pecuniaria di 1.032 euro.

Da allora, però, ancora silenzio. La Asl, infatti, non pagava la multa né faceva pervenire documenti atti a giustificare il suo comportamento.

Di qui la decisione del Garante di una ordinanza ingiunzione nei confronti della azienda sanitaria per il pagamento della sanzione, ordinanza che è opponibile dalla Asl entro trenta giorni davanti al giudice di pace.

15 aprile 2002 - Stop a diffusione dati alunni handicappati su Internet

Immediata cancellazione da un sito Internet delle informazioni sulle malattie di alcuni alunni handicappati. Riserva di ulteriori accertamenti per verificare la liceità e la correttezza delle operazioni di raccolta e di utilizzazione dei dati e per valutare altresì i provvedimenti definitivi da adottare, anche ai fini dell'eventuale denuncia di reato.

Questo, in sintesi, il provvedimento d'urgenza con il quale il Garante, su segnalazione di alcuni genitori, è intervenuto per bloccare l'ulteriore diffusione di dati sanitari pubblicati sul sito web di un centro di documentazione didattica, che aveva sede presso la succursale di una scuola media statale.

Alla segnalazione che lamentava, oltre la diffusione dei nominativi degli alunni portatori di handicap, anche la descrizione dettagliata delle patologie sofferte da ciascuno di essi, ha fatto seguito l'accertamento preliminare eseguito dall'Ufficio del Garante. Dagli ulteriori accertamenti effettuati poi in sede di ispezione è emerso che, consultando la pagina Internet, accessibile attraverso il sito di un centro di documentazione scolastico, erano conoscibili, da chiunque, varie patologie di persone individuate nominativamente o appartenenti a classi, che venivano citate, di istituti scolastici.

Nel provvedimento collegiale che ha disposto il blocco dei dati, il Garante ha evidenziato la possibile violazione di diverse disposizioni della legge sulla privacy, ed in particolare dell'art. 23 che vieta la diffusione di informazioni sullo stato di salute degli interessati quando non sia necessaria per finalità di prevenzione, accertamento e repressione dei reati. Ritenendo, inoltre, necessario intervenire con urgenza, vista la particolare natura dei dati sanitari rilevati ed il concreto rischio che la permanenza sul sito di informazioni dettagliate potesse produrre un pregiudizio rilevante per gli alunni handicappati, l'Autorità ha ordinato anche l'immediata rimozione dei dati dalla pagina web.

Il Garante si è riservato, comunque, di effettuare ulteriori accertamenti per verificare la liceità e la correttezza dell'operato del centro di documentazione.

La legge sulla privacy, recentemente modificata dal decreto legislativo 467/2001, stabilisce che chiunque non rispetti il provvedimento di blocco del Garante è punito con la reclusione fino a tre anni.