Concetti e aggiornamenti di privacy e sicurezza informatica in farmacia

Raimondo Villano

Il diritto di tenere segreti i propri dati personali, in particolare quelli "sensibili" che riguardano le condizioni di salute e la vita privata delle persone, è sempre più sentito da parte di tutti. Per questo motivo è stata varata la legge 675/1996 ed è stata istituita l'Autorità Garante per la protezione dei dati personali (art.30 legge 675/96).
Con la legge sulla privacy, in effetti, si vuole garantire, indipendentemente dalla volontà del singolo, una forma di riservatezza "fisiologica" delle informazioni di carattere sanitario. La legge 675/1996, dunque, va considerata indubbiamente con favore e rispetto giacché sostanzialmente diretta a migliorare la qualità della nostra vita civile.
Tuttavia, come non di rado accade, benché i principi ispiratori del combinato disposto legislativo siano totalmente condivisibili, nell'applicazione pratica ci si confronta e ci si scontra anche con problemi vari da risolvere. In taluni casi, inoltre, accade che sia la stessa legge, paradossalmente, a minacciare di risultare invasiva, cioè a penetrare nei gangli operativi della vita sociale, ponendo problemi non giustificati dalla tutela che si propone di realizzare[(1)].
Ciò è il risultato di due aspetti concorrenti: l'imperfezione normativa, in parte inevitabile data la difficoltà del compito, e l'affermarsi di interpretazioni troppo rigide, quasi "fondamentaliste", come se la tutela della privacy non fosse un obiettivo cui tendere con la flessibilità resa necessaria dalla complicata articolazione della nostra vita civile ma un valore assoluto cui officiare acriticamente.
In farmacia le non poche problematiche principali di privacy possono essere *summa capita* ricondotte al trattamento dei dati delle ricette, alla conservazione delle ricette, alla gestione (informatica o cartacea) dei dati, alle promozioni commerciali, alle statistiche di marketing, alla fidelizzazione della clientela, a taluni rapporti con i dipendenti, all'uso di taluni veicoli di promozione ed informazione.
Preliminarmente, però, occorre, chiarire i concetti di "trattamento dati" e "dati personali" nell'ambito della privacy.
Il **trattamento** è tutto ciò che può essere fatto con dei dati: raccolta, analisi, classificazione, ecc. Relativamente ai trattamenti è necessario avere ben chiara la distinzione fra questi e il (o i) database cui si riferiscono; una stessa congerie di dati può essere oggetto di trattamenti diversi nelle modalità e negli obiettivi. In pratica, il trattamento di dati derivante da obbligo di legge non è soggetto al consenso preventivo, mentre il trattamento dello stesso identico database per finalità di promozione commerciale è soggetto ad un regime di maggiore controllo.
I **dati personali** sono solo quelli che direttamente o indirettamente consentono di correlare certe informazioni ad una persona e, infatti, la legge non si applica ai dati anonimi o resi tali alla fonte. I dati "*Mario Rossi*" "*tonsillite*" e "*collutorio XY*", quindi, presi isolatamente non sono di alcun interesse per la legge mentre nel momento in cui i dati si trasformano in informazioni, ad esempio "*Mario Rossi ha la tonsillite e utilizza il collutorio XY*", la situazione cambia drasticamente. Nell'ambito dei dati personali, quelli "sensibili", cioè quelli idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale, sono soggetti ad una regolamentazione più rigida che prevede speciali modalità di acquisizione del consenso dell'interessato e l'autorizzazione del Garante per i dati[(2)].
Nella fattispecie di inosservanza del divieto del Codice per la protezione dei dati personali relativamente a taluni trattamenti da parte del datore di lavoro o del responsabile, per combinato disposto degli artt. 170 e 143, comma 1, lettera c) richiamato dall'art. 154, comma 1), lettera d) è prevista la reclusione da tre mesi a due anni.
Nell'universo normativo della legge 675/96 un articolo, il 15, è dedicato all'adozione delle **misure minime di sicurezza** il cui contenuto è definito nel D.P.R. 318/99. L'omessa adozione di misure di sicurezza è un reato perseguibile d'ufficio con una pena che nell'ipotesi semplice può arrivare a due anni di reclusione.
È, dunque, fondamentale fare il possibile per applicare in modo corretto i contenuti del DPR in questione.
Tra gli adempimenti principali cui ottemperare si ricordano: l'attivazione della parola chiave (*password*) per l'accesso ai dati custoditi in computer non collegati in rete; essa dovrà essere fornita dal titolare o dal responsabile all'incaricato che dovrà avere, se il sistema lo permette, la possibilità di sostituirla con un'altra nota a lui solo. Ciò significa utilizzare programmi di crittografia per proteggere le informazioni. In caso di pluralità di incaricati e pluralità di parole chiave, deve anche essere individuato il detentore della password. È bene ricordare che i codici di accesso riguardano i singoli dati e non il sistema; l'attivazione di codici di accesso personalizzati nel caso di computer collegati in rete; l'installazione sul pc di un software antivirus la cui efficacia deve essere verificata con cadenza almeno semestrale. Ciò va fatto se sono trattati dati sensibili e se i computer utilizzati per il trattamento sono accessibili mediante una rete di telecomunicazioni disponibile al pubblico; la verifica dell'effettiva cancellazione dei dati prima di riutilizzare floppy disk, nastri, ecc; la distruzione dei supporti incancellabili (cd-rom, dvd); la conservazione dei dati su supporto cartaceo per evitare l'accesso indiscriminato (archivi con serrature, stanze chiuse); se i dati sono sensibili, gli incaricati che devono effettuare il trattamento devono custodirli in contenitori dotati di serratura[(3)].
Altri accorgimenti consigliabili sono: la dotazione di un gruppo di continuità, quantomeno per consentire il corretto salvataggio dei dati in caso di *blackout*; l'impiego di un sistema di *backup* che consente l'effettuazione di copie di riserva. Possono essere utili strumenti come masterizzatori (che consentono di scrivere su CD-ROM) o *streamer* (unità a nastro che consentono la memorizzazione di grandi quantità di informazioni).

---

(1) Abstract da**:** Raimondo Villano, "*La gestione della sicurezza in Farmacia"*, Prefazione, con presentazione del Dr. Piero Renzulli, già Consulente per la Sicurezza presso le Nazioni Unite (Small Business, Longobardi Ed., pag. 222, aprile 2004 - presentata al Congresso Nazionale della Federazione Nazionale dei Farmacisti Italiani da "Cutolo & Vartuli" nel maggio 2004; Standard Edition, Led Web International Editore, pag. 264, Torino, presentata alla Fiera del Libro di Francoforte, ottobre 2004).
(2) Ibid.
(3) Ibid.

La protezione dal "furto" delle informazioni o dalla loro abusiva circolazione è sostanzialmente affidata all'uso di *password* per l'accesso ai dati. I *computer* possono essere dotati di svariate categorie di *password*, da quelle che ne bloccano l'accensione a quelle che impediscono il collegamento ad una rete a quelle che non consentono l'accesso a singoli dati. Se un computer non è collegato ad una rete può essere sufficiente predisporre una *password* in accensione che verrà comunicata soltanto alle persone che hanno necessità di accedere a quelle informazioni.
Se invece è presente una rete che collega soltanto postazioni presenti nello stesso ambiente (cosiddette LAN, *Local Area Network*) sarà compito degli amministratori di sistema (le persone che sovrintendono al funzionamento dell'infrastruttura) gestire i vari utenti in conformità alle norme. Se, poi, i dati sensibili vengono trattati con una rete "aperta al pubblico" cioè liberamente accessibile da chiunque, come una piazza, sono necessarie ulteriori precauzioni di natura tecnica. Per quanto riguarda i trattamenti manuali, infine, è necessario dotarsi di armadi blindati, scaffali metallici con serratura e, soprattutto, di un distruggi documenti[(4)].
Come è noto, poi, aziende private e amministrazioni pubbliche hanno avuto il termine del 30 giugno 2004 per adottare le nuove **"misure minime" di sicurezza**[(5)] introdotte dal Codice della privacy[(6)] entrato in vigore il 1 gennaio 2004 a salvaguardia dei dati personali contenuti negli archivi dei sistemi informatici e telematici e per redigere il **documento programmatico in materia di sicurezza (dps)** che contiene l'analisi dei rischi che incombono sui dati personali e le tutele da adottare per prevenire la loro distruzione, l'accesso abusivo e la dispersione ed è obbligatorio per chi raccoglie, utilizza e conserva dati sensibili o giudiziari. Dal 2005, poi, decorso il periodo transitorio connesso all'entrata in vigore del Codice della privacy, il termine per l'aggiornamento del dps è fissato al 31 marzo.
La **redazione del dps** prevede i trattamenti del titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati e della struttura operativamente preposta, nonché degli strumenti elettronici impiegati. Per ciascun trattamento vanno indicate le seguenti informazioni obbligatorie secondo il livello di sintesi determinato dal titolare: la *descrizione sintetica*, menzionando il trattamento dei dati personali attraverso l'indicazione della finalità perseguita o dell'attività svolta (ad esempio: fornitura di beni o servizi, gestione del personale, ecc.) e delle categorie di persone cui i dati si riferiscono (clienti o utenti, dipendenti e/o collaboratori, fornitori, ecc.); la *natura dei dati trattati*, indicando se tra i dati personali sono presenti dati sensibili o giudiziari; la *struttura di riferimento*, indicando la struttura (ufficio, funzione, ecc.) all'interno della quale viene effettuato il trattamento; la *descrizione degli strumenti elettronici utilizzati*, indicandone la tipologia; la *banca dati* (data base o archivio informatico), indicando le relative applicazioni in cui sono contenuti i dati (nel caso che uno stesso trattamento richieda l'utilizzo di dati che risiedono in più di una banca dati, le banche dati possono essere elencate); il *luogo di custodia dei supporti di memorizzazione*, indicandone il sito in cui risiedono fisicamente i dati e/o dove si trovano (sede centrale o periferica, fornitore di servizi, ecc.) gli elaboratori sui cui dischi sono memorizzati i dati, i luoghi di conservazione dei supporti magnetici utilizzati per le copie di sicurezza (nastri, CD, ecc.) ed ogni altro supporto rimovibile[(7)].
Sono, inoltre, indicazioni facoltative: la *tipologia di dispositivi di accesso*, cioè l'elenco e la descrizione sintetica degli strumenti utilizzati dagli incaricati per effettuare il trattamento (pc, terminale non intelligente, palmare, telefonino, ecc); la *tipologia di interconnessione*, cioè la descrizione sintetica e qualitativa della rete che collega i dispositivi d'accesso ai dati utilizzati dagli incaricati (rete locale, geografica, Internet, ecc).
In altra sezione del dps, poi, occorre descrivere sinteticamente l'*organizzazione* della struttura di riferimento, i *compiti* e le relative *responsabilità* in relazione ai trattamenti effettuati[(8)]. Va fatta, inoltre, un'*analisi dei rischi* che incombono sulla sicurezza dei dati, un *elenco degli eventi dannosi* nonché una *valutazione dell'impatto sulla sicurezza* (conseguenze e gravità in caso di danno)[(9)]. In una specifica sezione, poi, vanno riportate in forma sintetica le misure in essere e da adottare per il *contrasto dei rischi* individuati[(10)] nonché i criteri e le *procedure di ripristino dei dati* in caso di loro danneggiamento o di inaffidabilità della base dati[(11)]. In altre sezioni, infine, vanno fatti una *pianificazione degli interventi formativi* ed un *quadro delle attività affidate a terzi* che comportano il trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi[(12)].
Altra problematica che può essere di interesse per la farmacia è quella della **privacy policy del sito internet** nel caso in cui attraverso tale website si richiedano dati personali agli utenti che lo consultano (come, ad esempio, per fini commerciali o per invio di materiale informativo quale bollettini, cd-rom, newsletter, relazioni annuali, risposte a quesiti, atti e provvedimenti, ecc.). In tal caso, infatti, è opportuno che in una specifica pagina in rete sia resa a coloro che interagiscono con i servizi web un'*informativa*, ispirata alla Raccomandazione del 17 maggio 2001 n. 2/2001 del Gruppo delle Autorità Europee per la Protezione dei Dati Personali[(13)] nonché ai sensi dell'art. 13 del d.lgs. n. 196/03

---

(4) Ibid.
(5) Già previste dalla legge n.675/1996, sono l'insieme degli accorgimenti tecnici e organizzativi che l'azienda deve adottare per assicurare almeno il livello minimo di sicurezza per la protezione dei dati personali.
(6) Ha confermato la disciplina in materia di sicurezza dei dati personali introdotta nel 1996. In particolare, è stato ribadito il principio secondo cui le "misure minime" sono solo una parte degli accorgimenti obbligatori in materia di sicurezza. Il Codice ha però aggiornato l'elenco delle "misure minime" di sicurezza e ha indicato modalità di applicazione (allegato B del Codice). Analogamente a quanto avveniva in passato, le "misure minime" sono diverse a seconda che il trattamento sia effettuato o meno con strumenti elettronici o riguardi dati sensibili o giudiziari.
(7) Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS) - (Codice in materia di protezione dei dati personali art. 34 e Allegato B, regola 19, del d.lg. 30 giugno 2003, n. 196), Parte I - Istruzioni, Elenco dei trattamenti di dati personali (regola 19.1) - Contenuti; Informazioni essenziali.
(8) Guida operativa, regola 19.2.
(9) Ibid., regola 19.3.
(10) Ibid., regola 19.4.
(11) Ibid., regola 19.5.
(12) Ibid., regole 19.6 e 19.7.
(13) Istituito dall'art. 29 della Direttiva n. 95/46/CE.

del Codice in materia di protezione dei dati personali, per individuare alcuni requisiti minimi per la raccolta di dati personali on-line, e, in particolare, le modalità, i tempi, il luogo ed il "titolare" del loro trattamento e la natura delle informazioni che essi devono fornire agli utenti quando si collegano a pagine web, indipendentemente dagli scopi del collegamento. L'informativa, però, è *resa solo per il sito della farmacia e non anche per altri siti* web eventualmente consultati dall'utente tramite link dello stesso website.
Va specificato, ancora, se i dati personali forniti dagli utenti sono utilizzati al solo fine di eseguire il servizio o la prestazione richiesta e se ed in quali casi sono comunicati a terzi o diffusi.
Deve essere, inoltre, fornita informazione all'utenza nel caso in cui i *dati di navigazione*, nel corso del loro normale esercizio, siano acquisiti dai sistemi informatici e dalle procedure software preposte al funzionamento del sito *web* registrando alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet. Tali informazioni, che comunque non dovrebbero essere raccolte per essere associate a interessati identificati, per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti. In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente.
Questi dati, dunque, andrebbero utilizzati al solo fine di ricavare informazioni statistiche anonime sull'uso del sito e per controllarne il corretto funzionamento e dovrebbero essere cancellati immediatamente dopo l'elaborazione. Tali dati, però, potrebbero essere utilizzati per l'accertamento di responsabilità in caso di ipotetici reati informatici ai danni del sito: salva questa eventualità, i dati sui contatti web cautelativamente non dovrebbero persistere per più di sette giorni.
Il caso, invece, di *dati forniti volontariamente dall'utente* con l'invio facoltativo, esplicito e volontario di posta elettronica agli indirizzi indicati sul sito, comporta la successiva acquisizione dell'indirizzo del mittente, necessario per rispondere alle richieste, nonché degli eventuali altri dati personali inseriti nella missiva; in tale evenienza, specifiche informative di sintesi possono progressivamente essere riportate o visualizzate nelle pagine del sito predisposte per particolari servizi a richiesta.
Va specificato, poi, se viene fatto uso di *cookies* per la trasmissione di informazioni di carattere personale o se sono utilizzati i c.d. *cookies persistenti*, ovvero sistemi per il tracciamento degli utenti. L'uso di c.d. *cookies di sessione* (che non vengono memorizzati in modo persistente sul computer dell'utente e svaniscono con la chiusura del browser) dovrebbe essere strettamente limitato alla trasmissione di identificativi di sessione (costituiti da numeri casuali generati dal server) necessari per consentire l'esplorazione sicura ed efficiente del sito. I c.d. cookies di sessione utilizzati in genere nei siti evitano il ricorso ad altre tecniche informatiche potenzialmente pregiudizievoli per la riservatezza della navigazione degli utenti e non consentono l'acquisizione di loro dati personali identificativi.
Vanno, poi, garantiti i *diritti dei soggetti interessati* cui si riferiscono i dati personali: essi, infatti, devono poter ottenere in qualunque momento, ai sensi dell'art. 7 del d.lgs. n. 196/2003, la conferma dell'esistenza o meno dei medesimi dati e di conoscerne il contenuto e l'origine, verificarne l'esattezza o chiederne l'integrazione o l'aggiornamento o la rettifica ovvero la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge nonché di opporsi in ogni caso, per motivi legittimi, al loro trattamento.
L'informativa sulla privacy, inoltre, deve essere consultabile in forma automatica dai più recenti browser che implementano lo standard *P3P* ("Platform for Privacy Preferences Project") proposto dal World Wide Web Consortium (www.w3c.org). È opportuno a tal proposito, ancora, che si rendano il più possibile interoperabili le funzionalità del sito con i meccanismi di controllo automatico della privacy disponibili in alcuni prodotti utilizzati dagli utenti. Considerando che lo stato di perfezionamento dei meccanismi automatici di controllo non li rende attualmente esenti da errori e disfunzioni, è opportuno che la *"*Privacy Policy*"* del sito sia soggetta ad aggiornamenti (magari lasciando le varie versioni consultabili al medesimo indirizzo).
Altra situazione che in farmacia può divenire impegnativa concerne, poi, è l'impiego di **"Fidelity card[(14)]"**.
L'Autorità Garante ha emesso nel 2005 alcune regole per i programmi di fidelizzazione a garanzia per i consumatori (informazione adeguata, libera scelta del consumatore, obbligo del consenso per profilazione e direct marketing) e stabilendo che tali "carte di fedeltà" vanno rilasciate anche se il cliente non intende acconsentire ad eventuali iniziative di profilazione o di marketing. I clienti beneficiari di carte di fedeltà, inoltre, devono essere informati in maniera chiara ed evidente sugli scopi per i quali i loro dati personali sono raccolti e, se le informazioni personali sono usate anche per costruire profili di consumatori, per ricerche di mercato o per direct marketing, essi devono esprimere, liberamente e senza sollecitazioni, il consenso su tale uso[(15)].
L'informativa al cliente deve essere chiaramente evidenziata all'interno dei moduli di sottoscrizione ed essere agevolmente individuabile rispetto alle altre clausole del regolamento.

---

(14) Tramite esse sono attribuiti vantaggi di varia natura (sconti per l'acquisto di prodotti, premi o bonus correlati, priorità, servizi accessori, facilitazioni di pagamento), di regola in base al volume di spesa complessivo realizzato; il loro rilascio (spesso mediante compilazione di questionari) e la loro utilizzazione (con la registrazione di beni e servizi effettuati) comportano un trattamento di dati personali dei clienti e, a volte, dei loro familiari. Accanto a dati anagrafici sono spesso raccolte altre informazioni, ad esempio titolo di studio, professione, interessi, abitudini di consumo, modalità di acquisto etc. Tali informazioni, tuttavia, possono essere utilizzate, senza che gli interessati ne abbiano piena conoscenza e possano acconsentire al loro uso, anche per monitorare in dettaglio i loro comportamenti o le loro propensioni al consumo, per creare cioè "profili" individuali o di gruppo o per confrontare le loro abitudini di consumatori con altri clienti. In taluni casi sono trattati anche dati sensibili (salute, adesioni a partiti o religioni, scelte di vita etc.) il cui trattamento, di regola, non è lecito per gli scopi legati al rilascio delle carte o per il direct marketing.
(15) Bollettino del n. 58/febbraio 2005, 24 febbraio 2005.

In particolare, deve essere posta in evidenza l'eventuale attività di profilazione o di marketing evidenziando che, per questi ultimi due usi, il conferimento dei dati e il consenso sono liberi e facoltativi. Non è lecito condizionare l'adesione al programma di fidelizzazione all'espressione del consenso anche per l'uso di dati a scopi di profilazione e marketing.
Le aziende, ha poi stabilito il Garante, devono ridurre al minimo l'uso delle informazioni personali e devono comunque utilizzare solo informazioni pertinenti e non eccedenti.
In particolare, per quanto riguarda la *fidelizzazione*, viene stabilito che possono essere trattati, senza che sia necessario acquisire il consenso dell'interessato, solo dati necessari per attribuire i vantaggi connessi all'utilizzo della carta, cioè dati per consentire l'identificazione dell'intestatario e, di regola, i dati relativi al volume di spesa globale realizzato, senza riferimento al dettaglio dei singoli prodotti acquistati.
Per l'attività di *profilazione,* invece, occorre il consenso dell'interessato per il trattamento delle informazioni relative agli acquisti effettuati. Non è lecito utilizzare a fini di profilazione dati sensibili, con particolare riguardo a quelli relativi allo stato di salute. Riguardo all'attività di *marketing* possono essere raccolti, sempre con il consenso dell'interessato, i dati necessari all'invio di materiale pubblicitario o di comunicazioni commerciali.
Per quanto riguarda il *tempo di conservazione dei dati* personali dei clienti, relativi al dettaglio degli acquisti, l'Autorità ha stabilito che per quelli raccolti a fini di profilazione non può superare un anno, mentre per quelli raccolti a fini di marketing non può superare i due anni.
É obbligatorio, infine, adottare le necessarie *misure di sicurezza* per evitare rischi di manomissione, furto o perdita dei dati. Nel caso di uso dei dati a fini di profilazione è obbligatorio comunicare l'avvio del trattamento al Garante[(16)].
Un altro tema di cogente interesse in farmacia, poi, è quello relativo all'evenienza da parte del datore di lavoro di effettuare il **trattamento delle informazioni del dipendente di carattere personale strettamente indispensabili**[(17)] per dare esecuzione al rapporto di lavoro. Il titolare di farmacia deve individuare il personale che può trattare tali dati e assicurare idonee *misure di sicurezza* per proteggerli da indebite intrusioni o illecite divulgazioni.
Il *lavoratore deve essere informato* in modo puntuale sull'uso che verrà fatto dei suoi dati e gli deve essere consentito di esercitare agevolmente i diritti che la normativa sulla privacy gli riconosce (accesso ai dati, aggiornamento, rettifica, cancellazione etc). Entro 15 giorni dalla richiesta il datore di lavoro deve comunicare in modo chiaro tutte le informazioni in suo possesso. Senza consenso non si possono comunicare informazioni ad associazioni di datori di lavoro, di ex dipendenti o a conoscenti, familiari, parenti. Il *consenso* è necessario anche per pubblicare informazioni personali (foto, curricula) nella Intranet aziendale ed a maggior ragione in Internet. Nella bacheca aziendale possono essere affissi solo ordini di servizio, turni lavorativi o feriali. Non si possono, invece, diffondere emolumenti percepiti, sanzioni disciplinari, assenze per malattia, adesione ad associazioni.
I *dati sanitari* vanno conservati in *fascicoli separati*. Il lavoratore assente per malattia è tenuto a consegnare un certificato senza la diagnosi ma con la sola indicazione dell'inizio e della durata presunta dell'infermità. Il datore di lavoro non può accedere alle cartelle sanitarie dei dipendenti sottoposti ad accertamenti dal medico del lavoro. Nel caso di denuncia di infortuni o malattie professionali all'Inail, il datore di lavoro deve limitarsi a comunicare solo le informazioni connesse alla patologia denunciata.
Un'altra problematica che può essere interessante per la farmacia riguarda la **posta elettronica e la navigazione in Internet dei dipendenti** che i datori di lavoro privati non possono controllare, se non in casi eccezionali. In effetti, con riguardo al principio secondo cui occorre perseguire finalità determinate, esplicite e legittime (*art. 11, comma 1, lett. b), del Codice*), il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (*cfr. artt. 2086, 2087 e 2104 cod. civ.*). Spetta al datore di lavoro definire le modalità d'uso di tali strumenti ma tenendo conto dei diritti dei lavoratori e della disciplina in tema di relazioni sindacali. Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori[(18)]" (*art. 4, comma 1, l. n. 300/70*), tra cui sono certamente comprese strumentazioni hardware e software mirate al controllo dell'utente di un sistema di comunicazione elettronica.
Il trattamento dei dati che ne consegue, anche con i lavoratori consapevoli, è illecito, a prescindere dall'illiceità dell'installazione stessa. In particolare non può ritenersi consentito il trattamento con *hardware* e *software* preordinati al controllo a distanza, che consentono di ricostruire, a volte anche minuziosamente, l'attività di lavoratori.
Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (ad es., per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (*art. 4, comma 2*), di sistemi che consentono un *controllo indiretto a distanza* (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Ciò anche in presenza di attività di controllo discontinue. Il trattamento di dati che ne consegue può risultare lecito, restando ferma la necessità di rispettare le procedure di informazione e consultazione di lavoratori in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonchè in caso di introduzione o di modifica di procedimenti tecnici per controllare i movimenti o la produttività dei lavoratori.
Il Garante per la protezione dei dati personali, inoltre, con un provvedimento generale pubblicato sulla Gazzetta Ufficiale[(19)], ha prescritto ai datori di lavoro di informare con chiarezza e dettagliatamente i lavoratori sulle modalità di utilizzo di Internet e della posta elettronica e sulla possibilità che vengano effettuati controlli. Il Garante vieta, poi, la lettura e la registrazione sistematica delle e-mail ed il monitoraggio sistematico delle pagine web visualizzate dal lavoratore, perché ciò realizzerebbe un controllo a distanza dell'attività lavorativa vietato dallo Statuto dei lavoratori.

---

(16) Autority, doc. web n. 771307
(17) Maggiori garanzie sul posto di lavoro: le linee guida del Garante privacy - Principi generali - Roma, 13 dicembre 2006.
(18) Art. 4, primo comma, l. n. 300/1970.
(19) *Lavoro: le linee guida del Garante per posta elettronica e internet* - Reg. deliberazioni Del. n. 13 del 1° marzo 2007 - G. U. n.58 10.03.07.

Viene, inoltre, indicata una serie di misure tecnologiche ed organizzative per prevenire la possibilità, prevista solo in casi limitatissimi, dell'analisi del contenuto della navigazione in Internet e dell'apertura di alcuni messaggi di posta elettronica contenenti dati necessari all'azienda.
Il datore di lavoro, in effetti, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'*upload* o il *download* di *file*, l'uso di servizi di rete con finalità ludiche o estranee all'attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. Tali controlli, leciti o meno, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale (*art. 8 l. n. 300/1970; artt. 26 e 113 del Codice; Provv. 2 febbraio 2006, Garante*).
In particolare, il datore di lavoro può: individuare categorie di siti considerati correlati o meno con la prestazione lavorativa; configurare sistemi o utilizzo di filtri che prevengano determinate operazioni, quali l'accesso a siti inseriti in una sorta di *black list*, reputate inconferenti con l'attività lavorativa; eventualmente conservare nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.
Il provvedimento raccomanda l'adozione da parte delle aziende di un disciplinare interno, definito coinvolgendo anche le eventuali rappresentanze sindacali, in cui siano indicate le regole per l'uso di Internet e della posta elettronica.
Per quanto riguarda la posta elettronica, il contenuto dei messaggi, come anche i dati esteriori delle comunicazioni e i file allegati, riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui *ratio* risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti[(20)].
Tuttavia, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa.
Tra le soluzioni che possono risultare utili per contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonchè violazioni della disciplina sull'eventuale segretezza della corrispondenza, è opportuno che l'azienda: renda disponibili anche indirizzi condivisi tra più lavoratori (info@ente.it; urp@ente.it; ufficioreclami@ente.it), rendendo così chiara la natura non privata della corrispondenza; valuti la possibilità di attribuire al lavoratore un altro indirizzo (oltre quello di lavoro), destinato ad un uso personale; preveda, in caso di assenza del lavoratore, messaggi di risposta automatica con le coordinate di altri lavoratori cui rivolgersi; metta in grado il dipendente di delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi a lui indirizzati e a inoltrare al titolare quelli ritenuti rilevanti per l'ufficio, ciò in caso di assenza prolungata o non prevista del lavoratore interessato e di improrogabili necessità legate all'attività lavorativa.
Qualora queste misure preventive non sono sufficienti a evitare comportamenti anomali, gli eventuali controlli del datore di lavoro devono essere effettuati con gradualità. Inizialmente si individua l'area da richiamare all'osservanza delle regole e solo successivamente, ripetendosi l'anomalia, si potrebbe passare a controlli su base individuale.
La violazione dell'art. 114 del Codice, richiamandosi all'art. 4 dello Statuto dei Lavoratori, è fattispecie sanzionata penalmente dall'art. 171 del Codice per la protezione dei dati personali per il controllo a distanza dei lavoratori da parte dei datori di lavoro mediante registrazione sistematica dei messaggi di posta elettronica o effettuato mediante memorizzazione sistematica delle pagine web visualizzate dal lavoratore o ancora mediante la lettura dei caratteri inseriti tramite tastiera o attraverso l'analisi occulta del computer portatile affidato in uso.
Un'ultima casistica che potrebbe, in taluni casi, assumere una discrerta rilevanza anche in farmacia è quella dello *spamming*, ovvero l'**invio di fax, e-mail, sms e mms indesiderati**.
Per tale evenienza il Garante in un recente provvedimento ha vietato l'uso illecito di dati personali a fini di marketing a mezzo invio sistematico e ad una molteplicità di persone di materiale pubblicitario e comunicazioni commerciali senza il consenso dei destinatari. Nel definire il procedimento, il Garante ha ribadito che inviare fax commerciali senza il consenso informato dei destinatari[(21)] comporta un trattamento illecito e, ancor più, che lo spam può causare danni al destinatario. Nel caso di invio via fax tale danno può consistere, tra l'altro, nella perdita di tempo, nell'uso indebito della carta, del toner del suo apparecchio e nel disturbo per la comunicazione indesiderata che occupa l'apparecchio.
Benchè, inoltre, possa essere addotta a giustificazione da parte della farmacia che l'invio di fax commerciali sia limitato ai soli soggetti economici i cui numeri risultano reperibili sugli elenchi categorici[(22)] (Pagine gialle, Pagine utili), il Garante ha spiegato che anche in tal caso non vi è possibilità di un invio senza consenso quando le comunicazioni commerciali sono effettuate con le particolari modalità della via fax, posta elettronica, sms o mms o chiamate vocali mediante operatore automatico. Tali comunicazioni, infatti, sono considerate dal Garante oggi le forme più invasive di disturbo nella vita quotidiana di utenti e consumatori ed un fenomeno che va combattuto per liberare le reti di comunicazione da chi le ingolfa solo per proprio profitto. In questa "battaglia di civiltà" il Garante ha proceduto in maniera sempre più incisiva in difesa dei cittadini finanche ricorrendo ad ispezioni tramite Guardia di Finanza, denunciando alla magistratura i responsabili e comminando gravi sanzioni.
Né va comunque trascurata la considerazione, infine, che resta assolutamente impregiudicata la facoltà per gli interessati di agire in sede civile in relazione alla condotta invasiva accertata[(23)].

---

(20) Artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, comma 4, c.p.; art. 49 Codice dell'amministrazione digitale.
(21) Tale attività soggiace all'art. 130, comma 2, del Codice che prevede il necessario consenso informato, specifico e preventivo dell'interessato.
(22) Il provvedimento dell'Autorità Garante della privacy del 14 luglio 2005 doc. web n. 1151640 individua modalità e garanzie semplificate per la formazione degli elenchi telefonici organizzati per categorie merceologiche/professionali, prescrivendo alcune misure che devono essere adottate con particolare riferimento, rispettivamente, all'acquisizione e all'inserimento dei dati personali, nonché all'informativa da fornire agli interessati.
(23) Ai sensi dell'art. 15 del Codice, secondo il quale chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento del danno, anche non patrimoniale, ai sensi dell'art. 2050 c.c.