ALCUNI COMMENTI DALLA RETE SUL NUOVO "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI"

(Decreto legislativo n. 196 del 30 giugno 2003)

INTRODUZIONE

Internet è uno strumento di comunicazione sul quale transitano informazioni di vario tipo, in elevata quantità e su larga scala. Tale flusso di dati – potendo riguardare anche dati personali – pone necessariamente problemi in relazione alla tutela della privacy. Ciò deve essere ben compreso dall'azienda che si affaccia in Rete, rappresentando anzi questa considerazione il "dato di partenza" per l'impresa che voglia implementare la propria attività on line o comunque utilizzi Internet per consultazione o per la comunicazione con operatori economici (clienti, fornitori, banche, etc..). Il termine "privacy" è ormai divenuto parte del linguaggio corrente, stante la larga applicazione che ne viene fatta quotidianamente.

La parola "privacy" è certo nota a tutti, eppure non sempre viene correttamente intesa nel suo significato, specie se utilizzata in contesti giuridici. Un pregiudizio molto diffuso, sostiene che la legge sulla privacy introduca il "diritto all'anonimato". In realtà, la legge (articolo 1 del Testo Unico) sancisce il "diritto alla protezione dei dati personali", diritto peraltro già elevato a livello comunitario a diritto fondamentale della persona (vedi art. 8 della Carta dei diritti del cittadino europeo).

Altrettanto falso è che il rispetto della normativa sulla privacy sia d'ostacolo allo sviluppo di attività commerciali o comunque economiche. E' stato dimostrato che l'adottare politiche di riservatezza crea una relazione di fiducia con i consumatori, ragione per la quale le imprese devono prendere coscienza della necessità di gestire al meglio il flusso dei dati personali dei propri clienti.

Il rispetto della normativa in tema di "data protection", è per l'azienda davvero "una necessità", ormai non più procrastinabile. Soprattutto ora, dal momento che esiste un testo normativo che elenca dettagliatamente gli adempimenti cui è tenuto il soggetto che effettua trattamenti di dati personali altrui.

Il Testo Unico sulla privacy ("Codice sulla protezione dei dati personali"), attuato col Decreto Legislativo 30 giugno 2003 n. 196 (che entrerà in vigore il 1°gennaio 2004, abrogando – tra l'altro – la L.675/96 e il D.P.R. 318/99), introduce alcune modifiche che incideranno in modo rilevante sull'impianto normativo attuale della materia.

E' stata quanto mai opportuna la scelta di adottare un Testo Unico, creato ad hoc, per la disciplina di questa materia. Basti ricordare a tal proposito che dal 1997 in poi il processo di completamento del quadro normativo delineato dalla L.675/96 si è sviluppato attraverso 9 decreti legislativi e 2 D.P.R, nonché attraverso molte altre specifiche disposizioni, legislative e regolamentari, inserite in numerosi provvedimenti speciali.

L'adozione di un solo Testo Unico, permette di semplificare notevolmente l'impianto e la "leggibilità" delle norme in materia. Ma l'intero "Codice della privacy", può ritenersi il frutto di istanze più volte avanzate dagli operatori professionali e dalla stessa Autorità Garante, in termini di semplificazione degli adempimenti e di adozione di garanzie sostanziali e non meramente formali. Forse anche per questo, il Testo Unico non è meramente riepilogativo della disciplina attualmente vigente.

Esso è strutturato in 3 parti, così suddivise: a) una "parte generale", contenente disposizioni riguardanti le regole sostanziali della disciplina del trattamento dei dati personali, applicabili per lo più a tutti i trattamenti; b) una parte "speciale", dettata per casi specifici; c) una terza ed ultima parte, che disciplina la tutela giurisdizionale ed amministrativa concessa all'interessato, nonché il sistema sanzionatorio.

GLI "ADEMPIMENTI –PRIVACY"

L'Imprenditore che si propone di utilizzare il mezzo telematico quale strumento di comunicazione con la propria clientela, dovrà esaminare approfonditamente i singoli adempimenti da effettuare, per conformarsi alla normativa.

Diciamo subito che, in linea generale, tre sono gli adempimenti fondamentali che un'impresa è tenuta a porre in essere per poter correttamente procedere al trattamento dei dati personali:

- la notificazione al Garante;
- la comunicazione dell'informativa all'interessato;
- l'acquisizione del consenso.

ATTIVITA' PRELIMINARI

Un'attività che vuole utilizzare Internet e/o la Posta Elettronica come strumento di lavoro, deve preliminarmente procedere all'individuazione dei soggetti che a vario titolo hanno accesso ai dati trattati.

L'azienda infatti dovrà essere in grado di rispondere adeguatamente ad un'istanza avanzata in tal senso dall'interessato, al quale l'articolo 7 comma 1, lettera e) del Testo Unico, attribuisce il diritto di conoscere i soggetti ai quali i dati possono essere comunicati o che ne possono comunque venire a conoscenza.

L'impresa dovrà inoltre regolare "ai fini privacy" i rapporti con le altre società del proprio gruppo, o i rapporti con i propri partners commerciali (es. l'host provider che cura la gestione del server su cui è allocato il sito aziendale, l'asp in outsourcing, gli istituti bancari che gestiscono il pagamento on line da siti di e-commerce, ecc.).

Il titolare del trattamento, dovrà rivolgere particolare attenzione sulla necessità od opportunità di nominare i soggetti coinvolti nella gestione dei dati quali "responsabili" e/o "incaricati" del trattamento.

I dipendenti dell'azienda, se non sono nominati "responsabili" del trattamento, ma comunque trattano dati, assumono la qualifica di "incaricati" del trattamento. Il Testo Unico dedica un articolo apposito (art. 30) a quest'ultima figura, disponendo che essi debbano sempre operare sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. Il 2°comma precisa che la designazione va effettuata per iscritto e deve specificare puntualmente l'ambito del trattamento consentito.

L'impresa dovrà in via preliminare analizzare attentamente i flussi di dati "coinvolti" dal proprio business e procedere al meccanismo delle "nomine", a cui ne derivano le incombenze normative a cui ci si deve attenere per il relativo trattamento.

LA NOTIFICAZIONE

Cominciamo a parlare della notificazione (art. 37-38 Testo Unico), primo adempimento da porre in essere.

E'un adempimento di particolare importanza e da effettuarsi con la dovuta cura (il Testo Unico, infatti, all'articolo 163 prevede una sanzione amministrativa per l'omessa o incompleta notificazione e punisce come reato – cfr. l'art. 168 – la falsità nella notificazione).

La notificazione è un atto (una sorta di "auto-dichiarazione") con il quale il soggetto-impresa "si presenta" al Garante, portandogli a conoscenza che nell'espletamento della propria attività tratterà dati personali di terzi.

A differenza della precedente Legge 675/96, in cui dovevano notificare tutti i soggetti non esplicitamente esentati, col Testo Unico si rovescia l'impostazione e si indicano solo i pochi casi nei quali la notifica va effettuata. Alcuni di essi, sono comunque frequenti in ambito aziendale: così, ad esempio, deve notificare chi fa videosorveglianza, o chi utilizza dati sensibili per ricerche di marketing, o chi ancora si avvale di strumenti elettronici per la profilazione del consumatore (si pensi al sito aziendale che rilasci "cookies").

Rispetto alla normativa precedente diminuiscono le ipotesi di notifica obbligatoria e vengono snellite anche le modalità della notifica stessa, che sarà effettuata solo per via telematica, utilizzando la firma digitale (art. 38, co.2 T.U.).

L'INFORMATIVA

Esaminiamo ora come si struttura l'informativa che l'impresa deve dare all'interessato, le cui linee-guida sono contenute nell'art. 13 del Testo Unico.

Essa è un atto molto importante, il primo "obbligo-privacy" nei confronti dell'utenza, a differenza della notificazione che ha per interlocutore il Garante.

L'informativa è anzitutto un atto con il quale chi tratta dati personali altrui "si identifica" nei confronti dell'interessato, rendendogli note le caratteristiche del trattamento ed illustrando i diritti riconosciuti a quest'ultimo dalla legge.

L'informativa deve quindi contenere:

a) le finalità e le modalità del trattamento dei dati;
b) la natura obbligatoria o facoltativa del conferimento dei dati;
c) le conseguenze di un eventuale rifiuto di rispondere;
d) i soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza, e l'ambito di diffusione dei dati medesimi (questa indicazione è un obbligo di legge "nuovo", non previsto dalla L.675/96);
e) i diritti dell'interessato, come previsti dall'art.7 del Testo Unico;
f) gli estremi identificativi del titolare.

Va osservato, infine, che l'informativa è un atto che deve necessariamente precedere il trattamento dei dati ed è atto privo di particolari formalità, che va redatto in maniera chiara e sintetica.

IL CONSENSO

Per trattare i dati personali le imprese e, più in generale, i soggetti privati sono obbligati, salvo eccezioni espressamente previste, ad acquisire il preventivo consenso dell'interessato.

Dispone, infatti, l'art. 23 del Testo Unico, al primo comma, che "il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato".

Già dalla lettura del disposto testè citato si può ricavare una preziosa indicazione, che riguarda la modalità di espressione del consenso: il consenso deve essere espresso "positivamente".

Non è dunque efficace un consenso reso in forma implicita, o in forma negativa (cioè inteso come mera possibilità di esprimere un dissenso, barrando ad esempio una casella), forma – quest'ultima – per la verità piuttosto diffusa.

L'azienda che lo voglia richiedere on line, dovrà avere l'accortezza di inserire sul sito web un "bottone di consenso", sul quale occorre cliccare per attestare l'avvenuta autorizzazione al trattamento dei propri dati personali.

Il consenso – che deve essere "preventivo" rispetto all'utilizzo dei dati ("opt-in") – perché sia validamente prestato deve essere espresso "liberamente" e "in relazione ad un trattamento chiaramente individuato" (il consenso omnibus, dunque, viene visto come una sostanziale elusione del principio stesso del consenso), nonchè deve essere "informato" (ossia preceduto da una corretta informativa).

Si precisa, ancora, che qualora abbia ad oggetto dati sensibili, il consenso deve essere "rilasciato" per iscritto, mentre, in caso contrario, è sufficiente che sia "documentato" per iscritto (in quest'ultima ipotesi – verrebbe da dire - la forma scritta è sempre richiesta).

Il consenso dovrà poter essere revocato, in ogni momento, senza che l'interessato abbia la necessità di addurre una particolare ragione giustificativa.

Ovviamente, la revoca non inficia la liceità dei trattamenti già effettuati, ma ne comporta pur sempre la cessazione, in termini che non implicano solo l'interruzione delle operazioni, ma che interessano anche la sorte dei dati, i quali andranno dismessi, qualora non possano essere detenuti in virtù di altro titolo.

Solo un accenno alla sanzione, particolarmente incisiva, per chi effettui trattamenti senza consenso.

L'art. 167 del Testo Unico ricollega anche quest'ipotesi al reato di "trattamento illecito di dati", ove detto trattamento sia compiuto al fine di trarne profitto o di recare un danno, e semprechè – beninteso – dal fatto derivi nocumento. Detto reato è punito con la reclusione da 6 a 18 mesi.

3) LA POSTA ELETTRONICA IN AZIENDA

Andiamo ora ad analizzare alcuni aspetti per così dire "complementari" alla tematica del rispetto della privacy per l'impresa in Rete.

L'indagine ha ad oggetto la posta elettronica e il suo l'utilizzo "aziendale".

Si tratta, in buona sostanza, di esaminare due aspetti dell'e-mail, l'uno per così dire "interno", l'altro "esterno". Il compito consiste nel rispondere ai seguenti due interrogativi:

a) se il datore di lavoro abbia il potere di leggere la posta elettronica del dipendente;
b) se l'azienda possa inviare e-mails non sollecitate a terzi senza dar luogo a "spamming".

LA TUTELA DELL'E-MAIL AZIENDALE

L'articolo 5 della Legge 547/93, recita testualmente: "Per corrispondenza si intende quella epistolare, telegrafica o telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza".

La giurisprudenza amministrativa (cfr. T.A.R. Lazio, Sez. I, 15.11.01 n. 9425), del resto, ribadisce che la posta elettronica deve essere tutelata alla stregua della corrispondenza epistolare ed è quindi caratterizzata dalla "segretezza". Sulla stessa lunghezza d'onda è il Garante per la privacy, che in più occasioni ha avuto modo di precisare che le caselle di posta elettronica, le mailing list, i newsgroup chiusi (quelli, cioè, a cui si accede solo tramite ID & password) sono equiparati ai recapiti postali tradizionali (si veda sul punto la Newsletter 12-18.07.99).

Ne consegue che è vietato leggere i messaggi se non si è i destinatari, pena l'applicazione dell'art.616 c.p., secondo il quale "chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta…è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno". Vi è di più. Si punisce anche chi, oltre che prendere cognizione, sottrae, distrae la corrispondenza, la sopprime o la distrugge.

Se quanto precede è un quadro – pur se sintetico – della tutela che il nostro ordinamento accorda alla corrispondenza (e dunque, come abbiamo visto, anche a quella inviata o ricevuta tramite posta elettronica), quando si parla di "e-mail aziendale" bisogna fare attenzione. E molta, perché in azienda lo scenario è parzialmente diverso.

Prendiamo le mosse da un caso concreto, un caso che potrebbe definirsi "ordinario". Questi, in estrema sintesi, i fatti.

Ad un'impiegata viene assegnata, come a tutti gli altri dipendenti, una casella di posta elettronica aziendale (nome.cognome@azienda.it). Durante l'assenza per ferie dell'impiegata, la sua responsabile ne controlla la posta e si imbatte in comunicazioni inerenti progetti di lavoro "personali", estranei cioè a quelli gestiti dalla dipendente per conto dell'azienda.

Ravvisando in tale condotta una violazione dei doveri relativi al rapporto di lavoro, il responsabile della società licenzia l'impiegata. Essa, a sua volta, impugna il licenziamento e sporge contestuale querela nei confronti della propria responsabile, per il reato di cui all'art. 616 c.p. (violazione di corrispondenza).

Il P.M. però avanza richiesta di archiviazione. La dipendente propone allora opposizione, che viene tuttavia respinta dal GIP, con un'ordinanza particolarmente significativa, divenuta presto "celebre" perché la prima a prendere posizione sulla legittimità (o meno) dell'accesso del datore di lavoro alla mailbox del dipendente.

Sostiene il GIP (cfr. ordinanza GIP Tribunale di Milano del 10 maggio 2002) che quanto affermato nell'art. 616 c.p. non può trovare applicazione con riferimento all'ipotesi di e-mail aziendale.

La casella di posta elettronica, in altre parole, è sì tutelata, ma quando a metterla a disposizione è il datore di lavoro perde tutta la sua "riservatezza", in quanto strumento che l'azienda mette a disposizione del lavoratore al solo fine di consentirgli di svolgere la propria attività: come tale rimane nella completa e totale disponibilità del datore di lavoro, senza alcuna limitazione.

La mailbox aziendale - pur se "personale" (perché assegnata al singolo dipendente che ha un proprio "username" ed una propria "password" per accedervi) – deve quindi essere intesa come semplice "strumento di lavoro", e nulla più. "Personalità" non significa necessariamente "privatezza" dal momento che l'e-mail aziendale, proprio perché tale, rimane bene aziendale, accessibile a tutti gli altri dipendenti autorizzati, ed al datore di lavoro in primis.

LO SPAMMING "AZIENDALE"

Un rapido esame sulle "cautele" che l'azienda che invii a terzi posta elettronica a carattere commerciale deve osservare, per non essere accusata di "spamming".

E' noto che con tale termine si intende l'invio per posta elettronica di un messaggio indesiderato - spesso inviato a grandi liste di utenti - contenente materiale promozionale non richiesto. La tentazione per l'impresa di comportarsi in tal modo è spesso forte, essendo palesi i vantaggi: a costi irrisori si possono raggiungere in tempo reale tantissimi potenziali consumatori, variamente distribuiti nel mondo.

Prassi pertanto diffusissima in Rete, lo spamming è però un fenomeno invasivo e oneroso per il destinatario, il quale il più delle volte è inerme di fronte a tale "flooding" di messaggi.

Va rilevato, in particolare, che in tutti questi casi, l'utilizzo spesso massivo della posta elettronica comporta una lesione ingiustificata dei diritti dei destinatari, costretti ad impiegare diverso tempo per esaminare e selezionare, tra i diversi messaggi ricevuti, quelli attesi o ricevibili, nonché a sostenere i correlativi costi per il collegamento telefonico, oppure ad adottare "filtri", a verificare più attentamente la presenza di virus, o a cancellare rapidamente materiali inadatti a minori.

Detto fenomeno ha recentemente trovato anche da noi una puntuale regolamentazione normativa, che ha così potenziato la tutela per l'utente della Rete.

Stabilisce anzitutto l'art. 130 del Codice della privacy, al 1°comma, che l'uso di "sistemi automatizzati di chiamata" (e quindi: posta elettronica, fax, SMS, ecc.) per l'invio di materiale pubblicitario o di altre comunicazioni commerciali è consentito solo nei confronti di coloro che abbiano espresso preliminarmente il loro consenso (c.d. "opt-in").

Una prima indicazione, dunque, per l'impresa che voglia inviare e-mails promozionali: essa deve prima aver acquisito il consenso informato, del destinatario.

Tale disciplina non può essere elusa inviando una prima e-mail che, nel chiedere un consenso abbia comunque un contenuto promozionale oppure pubblicitario, oppure riconoscendo solo un diritto di tipo c.d. "opt-out" al fine di non ricevere più messaggi dello stesso tenore.

Al contrario, è opportuna e va incoraggiata la prassi di alcuni fornitori i quali, dopo aver ottenuto realmente un valido consenso dei destinatari, danno semplice conferma della sua manifestazione, attraverso un messaggio volto unicamente ad annunciare il successivo inoltro di materiale pubblicitario.

L'articolo 9 Decreto Legislativo 70/03, aggiunge che le comunicazioni commerciali non sollecitate trasmesse per posta elettronica devono, in modo chiaro ed inequivocabile, essere identificate come tali fin dal momento in cui il destinatario le riceve e contenere l'indicazione che il destinatario del messaggio può opporsi al ricevimento in futuro di tali comunicazioni.

Il rispetto degli obblighi di legge, quindi, impone all'impresa che voglia effettuare via e-mail comunicazioni commerciali di:

a) acquisire il previo consenso del destinatario, adeguatamente informato;
b) esplicitare in modo chiaro che la comunicazione è a carattere commerciale;
c) informare il destinatario sulla possibilità di non ricevere più dette comunicazioni;
d) fornire un idoneo recapito presso il quale l'interessato possa esercitare i propri diritti in tema di privacy.

Le sanzioni per i trasgressori sono assolutamente di prim'ordine, e – come ricordato anche dal Garante con suo comunicato del 3 settembre 2003 - vanno dalla "multa", in particolare per omessa informativa all'utente (fino a 90mila euro), alla sanzione penale (reclusione da 6 mesi a 3 anni).

E l'impresa – lo ha precisato il Garante – non può giustificarsi invocando l'articolo di legge (ora l'art. 24, 1°comma, lett.c) del Testo Unico), che esonera il titolare del trattamento dal richiedere il consenso dell'interessato ove i dati di quest'ultimo provengano da elenchi pubblici.

Gli indirizzi e-mail, infatti, non sono "pubblici", non provenendo né da pubblici registri, né da elenchi, atti o documenti formati o tenuti da un soggetto pubblico.

Essi, quindi, non sono liberamente utilizzabili da chiunque per il solo fatto di trovarsi in Rete (cfr. Newsletter 10-16.02.03 Parere 29.05.03, consultabile su sito del Garante www.garanteprivacy.it). Pertanto, non è lecito inviare messaggi non sollecitati ad indirizzi reperiti da newsgroups, da siti web o dalle "pagine Whois" (le quali indicano gli assegnatari di nomi a dominio).

LE MISURE DI SICUREZZA

Per potere tutelare la privacy dei soggetti a cui si "trattano i dati", occorre adeguare i propri sistemi informativi e le infrastrutture aziendali, a misure di sicurezza, che impediscano la perdita accidentale dei dati nonché l'accesso abusivo agli stessi.

Diciamo subito che tale esigenza, da quando esistono le connessioni Internet e gli scambi di Posta Elettronica, viene avvertita in maniera ancor più concreta che nel mondo reale. In Internet i messaggi e le informazioni in genere transitano liberamente da un computer all'altro, in modo tale che è tecnicamente agevole intercettarli. Le aziende che connettano il proprio sistema informatico alla rete Internet, quindi, devono proteggersi (in una rete ben protetta, infatti, solo le aggressioni più sofisticate – e quindi, statisticamente, le meno probabili – possono realmente mettere in crisi il sistema).

Il Testo Unico sulla privacy affronta il tema della sicurezza al Titolo V della Parte Prima.

Due, in particolare, le misure di sicurezza che vengono in rilievo: quelle definite "minime" e quelle definite "idonee".

Le prime, previste in via generale dagli artt.33 e ss. Del Testo Unico, sono in concreto individuate dal disciplinare tecnico di cui al c.d."allegato B" (che sostituisce il sistema delle "misure minime" del D.P.R. 318/99, emanato in attuazione dell'art.15 della L.675/96) e sono volte ad assicurare un livello minimo di

protezione dei dati personali. Un livello al di sotto del quale non si può scendere: il mancato rispetto di dette misure, infatti, ai sensi dell'art. 169 del Testo Unico costituisce reato, punito con l'arresto fino a 2 anni o con l'ammenda da 10.000 a 50.000 Euro.

Le seconde, invece, sono disciplinate dall'art. 31 sempre del Testo Unico (Obblighi di Sicurezza), che impone al titolare del trattamento dei dati personali di predisporre tutte le misure di sicurezza idonee a ridurre al minimo "i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".

A questo punto, un'importante osservazione: se l'adeguamento alle "misure minime" implica l'assenza di responsabilità penali, tale adeguamento non è sufficiente per affrancarsi da responsabilità civile qualora l'evoluzione tecnologica renda disponibili accorgimenti ulteriori che soddisfino le misure dichiarate "idonee".

Ciò perché – ai sensi dell'art. 15 del Testo Unico – "chiunque cagiona danno ad altri per effetto del trattamento dei dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile".

L'art. 2050 c.c., infatti, (norma alquanto rigorosa, dettata in tema di esercizio di attività pericolose) prevede che l'esercente l'attività pericolosa – e quindi, nel nostro caso, il titolare del trattamento - vada esente da responsabilità solo se riesca a dimostrare di aver adottato tutte le misure idonee ad evitare il danno (prova diabolica).

In caso contrario, ai sensi del 2°comma dell'art. 15 del Testo Unico, egli dovrà rispondere anche del danno non patrimoniale (come accaduto nel caso deciso dal Tribunale di Orvieto con sentenza 22.11.02 n. 254: fattispecie in tema di risarcimento dei danni morali sofferti da alcuni clienti di un Istituto bancario).

Come si può riscontrare facilmente, l'adeguamento alla previsione di legge appena citata (art. 2050 c.c.) è particolarmente difficoltoso. Secondo la giurisprudenza, infatti, può provare di aver adottato ogni misura idonea chi dimostri di aver rispettato "tutte le tecniche note" – anche solo astrattamente possibili – all'epoca del fatto (cfr. Tribunale di Milano, 19 novembre 1987, in Foro Italiano, 1988, I, 144).

Sebbene esistano siti web e newsgroups che diffondono quotidianamente le vulnerabilità dei sistemi che vengono via via scoperte e, di conseguenza, illustrano i più recenti rimedi per difendersi dagli "attacchi informatici", per l'azienda la soluzione migliore per garantire la sicurezza del proprio sistema informatico è quella di affidarsi a professionisti del settore.

Riassumendo, l'impresa che adotti connessioni Internet utili alla propria attività, al fine di "ridurre i rischi", dovrà:

a) osservare il livello di sicurezza minimo di legge (per evitare conseguenze penali);

b) approntare le misure di sicurezza ulteriori, che in base al caso concreto si potevano predisporre (altrimenti dovrà risarcire i danni eventualmente cagionati a terzi).

IL SISTEMA SANZIONATORIO

Terminiamo dando uno sguardo al sistema sanzionatorio, al quale è dedicato l'intero Titolo III della Parte III del Codice della Privacy.

Il Capo I, in particolare, definisce le violazioni amministrative. Rispetto alla disciplina precedente, va notato non tanto che l'importo delle sanzioni è stato adeguato alla nuova moneta dell'euro, ma quanto che detto importo è stato opportunamente ricalibrato rispetto alla gravità delle violazioni.

Nell'applicazione della Legge 675/96, infatti, in più casi la particolare esiguità delle sanzioni non costituiva in concreto un efficace deterrente.

Il Capo II prende invece in rassegna le condotte integranti illeciti penali, quali – ad esempio – il trattamento dei dati in assenza di consenso, il mancato adeguamento dei sistemi informatici alle misure minime di sicurezza, l'uso di comunicazioni elettroniche indesiderate).

Non va dimenticato, in questa sede, l'articolo 15 del Testo Unico, che obbliga chi cagiona danno ai terzi per effetto del trattamento di dati personali a risarcire i danni sofferti, ivi compenso il danno non patrimoniale.

Sotto questo profilo è importante ricordare all'impresa che tratti dati personali, con una connessione interna ad Internet, che la potenziale diffusione degli stessi senza barriere amplifica il pregiudizio che l'interessato può subire, facendo lievitare l'importo dell'indennizzo.

Ci sono quindi "buoni" motivi perché l'azienda prenda coscienza delle indicazioni di legge e vi si conformi.

E' indubbio che l'adeguamento alla normativa vigente richieda uno sforzo, che spesso viene visto con sfavore dagli operatori.

Sono comunque maturi i tempi perché l'azienda possa capire che la tutela della privacy non è solo un aumento dei costi di gestione, ma che l'adottare politiche di riservatezza dei dati rappresenta invece un valore aggiunto al proprio prodotto o servizio.

La privacy, insomma, da "costo" deve essere vista come "risorsa": è questo il salto culturale che attende oggi l'impresa. E questo vale ovviamente anche per l'azienda presente utilizza i canali Internet all'interno dei propri processi economici.

Ciò non limita assolutamente il ricorso ad Internet, ma al contrario fa parte degli elementi fondamentali volti ad assicurare la fiducia degli utenti nell'impresa che utilizza i canali della rete come componenti essenziali nell'erogazione dei suoi servizi /prodotti.