LA LEGGE PER TUTTI
INFORMAZIONE E CONSULENZA LEGALE

Come rispettare la privacy nelle imprese

Autore: Redazione | 05/11/2013

Il Garante della privacy ha presentato un vademecum per venire incontro alle domande di aziende e imprenditori, preoccupati delle possibili responsabilità penali in caso di mancato rispetto della riservatezza della clientela.

Più si sviluppano le nuove tecnologie, maggiori sono le quantità di dati che ogni giorno vengono registrate, conservate ed utilizzate. Queste enormi masse di dati sono una **risorsa preziosissima** per tutti gli operatori economici, soprattutto per le imprese.

Sapere sfruttare al meglio i dati del proprio parco clienti o dei potenziali nuovi clienti è fondamentale, ma altrettanto importante è sapere che i dati vanno trattati nei modi e con le misure previste dalla legge **[1]**.

Per cercare di fornire un nuovo supporto alle imprese, è intervenuto, qualche mese fa, il **Garante** della privacy fa con un vero e proprio **vademecum**, dieci semplici regole che illustrano **problemi e possibili soluzioni** in tema di privacy **[2]**.

La prima indicazione del garante è quella sui **dati**. Sapere raccogliere al meglio i dati è un grande valore per l'azienda, ma bisogna sapere di cosa si parla. Per questo, i dirigenti e chi si occupano della raccolta, gestione e uso dei dati **[3]** devono conoscere la distinzione fondamentale tra dati **personali** e dati **sensibili**. I primi sono ad esempio il codice fiscale, il numero IP e quello di telefono; invece i dati sensibili sono, per esempio, quelli dai quali si può comprendere l'origine razziale, la convinzione religiosa o l'appartenenza ad un partito.

A fianco a questa distinzione vi sono poi altri tipi di dati che richiedono comunque particolari cautele, come i **dati giudiziari** (ad esempio quelli legati alle pendenze giudiziarie penali) o quelli **biometrici** (come le impronte digitali).

Come seconda indicazione si definiscono i ruoli **[4]** all'interno dell'azienda. Si parla così di **titolare del trattamento** e cioè di chi decide su fini e modi del trattamento. Può essere una persona fisica o una persona giuridica ed è, in pratica, colui che esercita direttamente il potere di gestione sui dati.

A fianco al titolare, specie nelle realtà aziendali più grandi, si può individuare, con atto scritto, un **responsabile del trattamento**. Questi avrà il compito di vigilare sul puntuale rispetto della normativa sulla privacy. Va specificato che il responsabile (persona fisica o persona giuridica) si affianca al titolare, ma che la sua nomina è **facoltativa**. Spesso si tratta di un soggetto esterno all'azienda, **specializzato nel settore**.

Infine vi è l'**incaricato del trattamento** e cioè la persona che è materialmente addetta alle operazioni di trattamento dei dati. Anch'esso va nominato per iscritto ed agisce seguendo le direttive del titolare o del responsabile.

Il terzo punto riguarda i **rapporti con i clienti**. Qui i capisaldi sono dati dall'informativa e dal consenso **[5]**.

L'**informativa** serve a spiegare dove si prendono i dati, per quale motivo si raccolgono, l'uso che se ne farà e a chi saranno o potranno essere forniti. In questa fase, maggiore è la **trasparenza** e la **semplicità** migliore sarà anche il feeling con il cliente. Chiunque, infatti, si insospettirebbe di fronte ad una richiesta dati criptica e complessa, mentre probabilmente di fronte ad una informativa semplice e chiara i dati saranno forniti con più tranquillità.

Proprio per ragioni di semplicità, l'informativa può essere **scritta** o anche **orale**. Addirittura, proprio per evitare che l'informativa si trasformi in un adempimento impossibile per l'impresa, il Garante consente **forme semplificate** di comunicazione, come ad esempio un **cartello** che indichi il fatto che la zona è videosorvegliata, le finalità della ripresa ed il nome del responsabile cui richiedere informazioni sul punto.

Dall'altra parte vi è il **consenso** che deve essere **informato** e cioè **chiaro** ed indicare per quale fine si raccolgono i dati. Il tipo di consenso da richiedere (genericamente per iscritto) varia molto in relazione al tipo di attività che si intende svolgere con i dati, ma vi sono specifici casi, previsti dalla legge, in cui si può procedere anche **senza il consenso**. Un esempio è dato dagli alberghi che, per legge, devono dare alle autorità di pubblica sicurezza le generalità delle persone che alloggiano nei propri edifici.

In alcuni casi, in cui si trattano dati di maggiore importanza, può essere anche richiesta una specifica **autorizzazione del Garante**, che consente all'impresa di agire in tutta tranquillità.

Un altro punto viene dedicato alla questione, spesso tralasciata dei **curricula**. Qui la distinzione sta nel fatto che sia l'azienda a chiedere il curriculum o sia il candidato a presentarlo spontaneamente.

Nel primo caso infatti, per aiutare al massimo l'incontro tra domanda ed offerta di lavoro l'impresa è **esonerata dall'obbligo** di dover rendere l'informativa vista al punto precedente.

Nel caso di **autocandidatura**, invece, se l'azienda dà seguito alla presentazione del curriculum e contatta il candidato gli deve fornire, anche in via semplificata, l'informativa.

E' per questo motivo che è buona norma chiudere il proprio curriculum con **l'autorizzazione espressa al trattamento** dei propri dati.

Il quinto punto contiene un obbligo per le imprese e cioè la **notificazione [6]** al Garante. Tramite questa comunicazione si forniscono **informazioni all'autorità** sul fatto che è iniziato un trattamento di dati che vengono considerati dalla legge particolarmente meritevoli di tutela, come ad esempio i dati genetici o quelli che forniscono una localizzazione geografica. Sul sito del Garante della privacy è possibile visionare, tramite un registro pubblico, tutte le notificazioni inviate.

Un punto poi delicatissimo riguarda il difficile rapporto tra nuove tecnologie e tutela della privacy. Nessuno vieta infatti all'imprenditore di dotarsi, ad esempio, di un sistema di telecamere di **video sorveglianza** in grado di tutelarlo al meglio di fronte al rischio di effrazioni, furti o rapine. Non vi sono limitazioni neppure per quello che riguarda la possibilità di introdurre all'interno dell'azienda un **software che ottimizzi la produzione** ed i contatti tra gli uffici. Tuttavia queste soluzioni devono fare i conti con la disciplina sulla privacy e con lo **Statuto dei lavoratori [7]**. È necessario **evitare**, in particolare, che tali strumenti diventino un **sistema di controllo a distanza** dei propri dipendenti, violandone così i diritti.

Proprio per evitare conflitti tra norme, il Garante richiede alle imprese che vogliono dotarsi di un sistema in grado di raccogliere e trattare i dati personali dei propri dipendenti, una **verifica preliminare** dei sistemi, in grado di fornire subito all'impresa una risposta circa la **legittimità** o meno dei mezzi tecnici che si vogliono adottare.

L'ottica che persegue l'autorità è quella di un **bilanciamento** tra tutela dei diritti

ed esigenze aziendali.

Anche il settimo punto cerca di tutelare al massimo le imprese, soprattutto nelle **situazioni di crisi**. È chiaro infatti che i dati raccolti costituiscono un rilevante valore per l'impresa che, ovviamente, deve fare in modo di non farsi sottrarre tale valore. I dati, cioè, vanno **conservati con cura** prevenendo, nei limiti del possibile, distruzioni, perdite o furti. Se questo risulta assai più semplice nel caso in cui trovi di fronte ad atti conservati su **supporti cartacei** (può bastare, ad esempio, chiuderli in una cassaforte), ben più difficile è la situazione nel caso di dati conservati su **supporti informatici**.

Per cercare di aiutare le imprese nella propria attività il Garante ha indicato una serie di **misure di sicurezza [8]** da adottare per assicurare un buon livello di tutela dei dati raccolti.

In particolare, si parla di **misure minime** e di **misure idonee**. Le prime sono gli accorgimenti minimi che debbono essere sempre adempiuti al fine di garantire la tutela dei dati ed evitare spiacevoli conseguenze all'impresa, ad esempio stabilendo un **sistema di controllo degli accessi** ai dati e la predisposizione di backup di sicurezza.

Il secondo gruppo di misure, invece, fornisce una tutela ulteriore, nei casi specifici in cui sia necessario adottare soluzioni più avanzate in relazione alla mole o all'importanza dei dati.

Va anche segnalato come il Garante sia in grado di fornire, su **propria iniziativa**, indicazioni sulle misure migliori da applicare nel caso concreto. Un controllo particolare, in questo momento, viene dato ad esempio alla disciplina del **cloud computing** e dei **rifiuti elettronici** (hard disk, chiavette, schede di memoria).

La successiva indicazione viene fornita, principalmente, alle **imprese di maggiori dimensioni**, nelle quali si traccia la figura dell'**amministratore di sistema** e cioè di colui che si occupa materialmente della gestione dei sistemi informatici e di quelli di sicurezza. Data la particolare tutela che la legge fornisce ai dati, si richiede che il soggetto che svolge quest'incarico sia **professionalmente**

qualificato e che il suo operato sia **chiaro e trasparente**. Per evitare, inoltre, che questo soggetto abusi della propria posizione si prevede anche un sistema di **registrazione degli accessi** e una **verifica**, con cadenza almeno annuale, **dell'operato** di tali amministratori da parte del titolare del trattamento.

Ovviamente tale regolamentazione non si applica nei casi di imprese di più modeste dimensioni.

La nona indicazione riguarda il **trasferimento dei dati**. Proprio come un materiale prezioso e molto sensibile ai danni, anche il dato raccolto, nel caso del suo trasferimento da luogo ad un altro, deve essere trattato con tutti i riguardi.

Se, ad esempio, un'impresa deve trasferire i propri dati da un paese europeo ad un altro, dovrà rispettare alcune **norme**, stabilite dall'unione europea, circa il **trasferimento sicuro**. Genericamente, comunque, la **circolazione dei dati** all'interno dell'unione europea è libera. Maggiori problemi sussistono, invece, nel caso in cui si debbano trasferire i dati in paesi al di fuori dell'unione. Il Garante ha predisposto un **elenco di paesi ritenuti affidabili**, perché già in possesso di una disciplina che garantisce una protezione uguale a quella nostrana. Con gli Stati Uniti, ad esempio, esiste uno **specifico accordo [9]** che garantisce la tutela dei dati.

La decima ed ultima indicazione riguarda la **rapidità**. Un'azienda in grado di rispondere rapidamente alle esigenze dei propri clienti si presenta meglio sul mercato, anche in relazione alla tutela dei dati personali.

Dal momento che l'interessato ha sempre la facoltà di poter accedere, rettificare, aggiornare o modificare i propri dati, un'azienda in grado di rispondere rapidamente a questa richiesta otterrà sicuramente un miglior profilo sul mercato. Dall'altra parte, anche ricordando le misure di sicurezza da adottare, un'azienda in grado di identificare in fretta i problemi nel caso di smarrimento o furti di dati, sarà in grado di informare tempestivamente i propri clienti dell'accaduto. Questo è molto importante soprattutto data l'enorme diffusione di una serie di nuovi **reati informatici**, come, ad esempio, la sostituzione di persona attuata con dati rinvenuti sulla rete.

Dimostrare la propria **rapidità e capacità di intervento** è sicuramente un valore aggiunto per ogni impresa.

di ANDREA PASSANO

Note

[[1]] La normativa di riferimento è data dal Decreto Legislativo numero 196 del 30/06/03. **[2]** Il documento è reperibile liberamente all'indirizzo http://www.garanteprivacy.it/documents/10160/2416443/Vademecum-privacy-e-imprese.pdf **[3]** Che vengono definiti titolari del trattamento dall'art. 4 del Decreto Legislativo numero 196 del 30/06/03. **[4]** Previsti dall'art. 4 del Decreto Legislativo numero 196 del 30/06/03. **[5]** Articoli 13 e 23 del Decreto Legislativo numero 196 del 30/06/03. **[6]** Art. 37 del Decreto Legislativo numero 196 del 30/06/03. **[7]** Legge numero 300 del 20/05/70. **[8]** Art. 31 del Decreto Legislativo numero 196 del 30/06/03. **[9]** Definito, simbolicamente, Safe Harbor (Porto Sicuro).