SAEV

Informa

Il Garante
il Piano ispettivo

Cloud computing
l'utilizzo consapevole dei servizi

Il web
siamo tutti spiati

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

La tutela dei dati personali: IL PRIMO GARANTE SEI TU.

www.garanteprivacy.it

S o m m a r i o

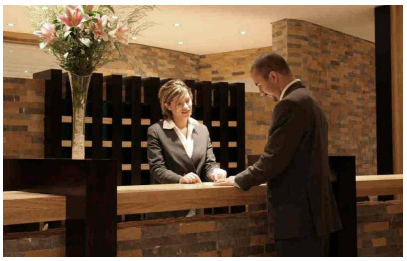
Edizione 2011 - Secondo Semestre

Interventi del Garante della Privacy

5

Piano ispettivo del garante per il secondo semestre 2011

Le regole Privacy per gli hotels



6

In Primo Piano

13

Redditi online: contrario alla pubblicazione delle dichiarazioni il Garante della Privacy.

La multa può essere annullata se il comune non redige il Dps

15

Privacy & Web

22

Il Web ci guarda: siamo tutti spiati

Sicurezza sul Lavoro

27

Il mestiere e la cassetta degli attrezzi del RLS

Corsi Saev

Corso Sicurezza sul Lavoro

32

Corso Privacy

33

Piano ispettivo del garante per il secondo semestre 2011

Telemarketing, uso massivo di fax indesiderati, attività di customer care, società di recupero crediti, enti previdenziali. E' su questi settori e sulle modalità con le quali vengono trattati i dati personali di milioni di cittadini italiani che punterà l'azione di controllo e accertamento del Garante per la privacy nei prossimi sei mesi dell'anno.

Il piano ispettivo appena varato prevede specifici controlli, sia nel settore pubblico che in quello privato, anche riguardo alle informazioni da fornire ai cittadini sull'uso dei loro dati personali, all'adozione delle misure di sicurezza, ai tempi di conservazione dei dati, al consenso da richiedere nei casi previsti dalla legge, all'obbligo di notificazione al Garante. Oltre 225 gli accertamenti ispettivi programmati che verranno effettuati come di consueto anche in collaborazione con le Unità Speciali della Guardia di Finanza - Nucleo Privacy.
A questi accertamenti si affiancheranno quelli che si renderanno necessari in ordine a segnalazioni e reclami presentati.

Un'attenzione particolare sarà data al contrasto del fenomeno della violazione del diritto di opposizione dei cittadini che si iscrivono al Registro recentemente istituito presso il Ministero dello sviluppo economico. Questo fenomeno, che nei primi mesi dell'anno ha visto un forte incremento di segnalazioni da parte di cittadini oggetto di chiamate indesiderate, sarà posto al centro dell'attività ispettiva e sanzionatoria dell'Autorità. Saranno infatti ispezionate dal Nucleo privacy della Guardia di finanza le società più segnalate per verificare la liceità dei loro trattamenti e, in caso contrario, applicate le sanzioni previste dalla legge.

Francesco Pizzetti, AutoritàGarante della Privacy.

Foto: impresamia.com

Intanto, un primo bilancio sull'attività ispettiva relativa al primo semestre 2011 mostra l'impegno dedicato dall'Autorità all'attività di verifica del rispetto delle norme sulla protezione dei dati personali: sono state circa 230 le ispezioni effettuate e 181 i procedimenti sanzionatori, relativi in larga parte alla omessa informativa, al trattamento illecito dei dati, alla mancata adozione di misure di sicurezza, all'inosservanza dei provvedimenti del Garante. Le ispezioni hanno riguardato in particolare le agenzie investigative, il settore sanitario, l'attività di profilazione on line, il telemarketing, il commercio elettronico.

Sempre nei primi sei mesi dell'anno le segnalazioni all'autorità giudiziaria per violazioni penali sono state 13, e hanno riguardato, tra l'altro, la mancata adozione di misure di sicurezza, la falsità nelle dichiarazioni e nelle notificazioni, il mancato adempimento ai provvedimenti del Garante.
Complessivamente le entrate derivanti dalle sanzioni sono state pari a circa 1 milione e 160 mila euro.

Le regole Privacy per gli hotels

Le schede che albergatori e gestori di pensioni compilano all'arrivo dei clienti, una volta inviate alle autorità di pubblica sicurezza, non devono essere conservate. I soli dati da conservare sono quelli a fini fiscali e contabili. Sulle schede devono essere riportate solo le generalità, non la residenza del cliente e la data di arrivo. Ma soprattutto occorre rivedere le norme che prevedono la raccolta generalizzata dei dati dei cittadini italiani che alloggiano in albergo.

É quanto chiede il Garante (Francesco Pizzetti, Giuseppe Chiaravalloti, Mauro Paissan, Giuseppe Fortunato) nel parere fornito al Ministero dell'interno su uno schema di decreto che regola le modalità per trasmettere alle questure i dati delle persone che alloggiano negli alberghi, in particolare attraverso reti telematiche.

Questi i punti essenziali del parere, di cui è relatore Giuseppe Fortunato (v. dichiarazione).

Le c.d. "schedine d'albergo", compilate per esigenze di polizia all'arrivo dei clienti, una volta assolto l'obbligo di comunicare i dati alle autorità di pubblica sicurezza tramite computer o su carta, non devono essere conservate. Il testo unico delle leggi di p.s. del 1931 non prevede questa conservazione. Albergatori, gestori di pensioni, appartamenti per vacanze, affittacamere, gestori di campeggi, ecc.. possono conservare solo dati eventualmente necessari a fini fiscali e contabili (ad esempio, informazioni da inserire nella fattura o ricevuta).

Per quanto riguarda la possibilità di trasmettere i dati mediante un collegamento via Internet, sono necessarie maggiori garanzie nel processo di certificazione dell'identità digitale del sito che riceve i dati, in modo da assicurare all'albergatore che il destinatario della comunicazione sia effettivamente la questura.

La consegna dei dati alle autorità di p.s. dovrà essere "diretta", specie per le schede cartacee, senza il tramite di altri enti o soggetti.

I dati raccolti presso uffici ed organi di polizia devono essere, comunque, conservati separatamente da altri dati personali detenuti per finalità di pubblica sicurezza e giustizia e deve essere previsto un termine breve di conservazione.

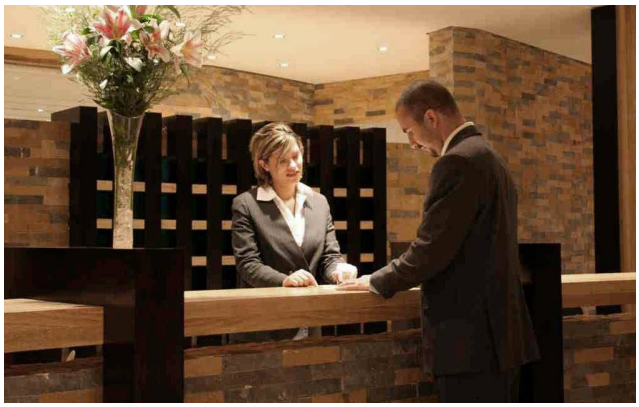


Foto: direttanews.it

I dati devono essere conservati solo presso le questure: per il Garante non è giustificato anche il loro inserimento in una banca dati centralizzata quale il C.e.d. del Dipartimento della pubblica sicurezza. Necessario, poi, individuare con precisione i soggetti che possono accedere alle informazioni.

Nel parere il Garante sollecita anche una verifica sulla necessità e proporzionalità di una misura che prevede la raccolta dei dati di tutti i cittadini italiani che alloggiano negli alberghi e in altri luoghi di soggiorno, ora che è intervenuto il Codice sulla protezione dei dati (entrato in vigore nel 2004) e tenuto conto che la Convenzione applicativa dell'Accordo di Schengen obbliga a rilevare per fini di polizia solo i dati relativi agli stranieri, anche europei, che soggiornano in alberghi e non anche quelli dei cittadini italiani. La Convenzione prevede, peraltro, che questi dati debbano essere trasmessi alle autorità di polizia solo se ciò è necessario per prevenire o accertare reati.

Il Garante, infine, rileva l'esigenza che venga adottato un decreto ministeriale che, dando ordine alla materia e certezza agli operatori nell'applicazione delle norme, sostituisca i precedenti decreti, alcuni dei quali abrogati o adottati senza il previsto parere del Garante, che si sono stratificati nel tempo.

Giustizia: il Garante privacy fissa le regole per la mediazione civile

L'Autorità garante per la protezione dei dati personali, ha emanato un provvedimento per semplificare procedure e adempimenti da parte degli organismi di medizione civile siano essi pubblici o privati, e fornito due autorizzazioni generali per autorizzare il trattamento dei dati sensibili e giudiziari che questi organismi trattano nell'esercizio delle loro funzioni.

L'intervento del Garante si è reso necessario perché la mediazione comporta l'uso dei dati personali delle parti che si avvalgono della conciliazione e degli altri eventuali protagonisti coinvolti nel procedimento, anche di tipo sensibile (ad es. richieste di risarcimento del danno da responsabilità medica o diffamazione) e giudiziario (ad es. dati relativi a sentenze di condanna penale in base alle quali si può chiedere il risarcimento).

Per essere in regola con la normativa i soggetti pubblici che intendono costituire un organismo di mediazione dovranno quindi rispettare la normativa sulla privacy e aggiungere al proprio regolamento per il trattamento dei dati sensibili e giudiziari un documento predisposto

Foto: as-live.com

dall'Autorità in cui sono individuati i tipi di dati (stato di salute, vita sessuale, convinzioni politiche, condanne ecc.) e le operazioni eseguibili (raccolta presso l'interessato o presso terzi, elaborazione in forma cartacea o automatizzata ecc.).
Il regolamento, integrato dal documento, non dovrà essere così sottoposto nuovamente al parere del Garante.

Linee guida del Garante per gli organismi sanitari che svolgono indagini sulla qualità dei servizi offerti ai cittadini

Il garante ha fissato delle regole alle quali dovranno attenersi gli organismi sanitari che svolgono indagini sulla qualità dei servizi offerti ai cittadini.

- I sondaggi possono riguardare esclusivamente informazioni sulla qualità del servizio (accoglienza, tempi di attesa, informazioni ricevute, confort della struttura) senza entrare nella valutazione degli aspetti sanitari delle prestazioni o delle cure erogate.
- I sondaggi non potranno riguardare dati sulla vita sessuale.
- Le informazioni raccolte tramite i sondaggi non potranno essere utilizzate per effettuare attività di profilazione o per l'invio di materiale pubblicitario.
- La partecipazione al sondaggio deve essere facoltativa.
- L'eventuale comunicazione o diffusione dei dati potrà avvenire solo in forma anonima o aggregata.
- Gli organismi sanitari saranno tenuti a richiedere un consenso scritto qualora le risposte fornite al sondaggio potranno rivelare informazioni sulla salute dell'utente, desumibili dal tipo di reparto che ha erogato il servizio.
- Agli utenti dovrà essere sempre assicurata una dettagliata informativa in cui risultano in chiaro tutti gli aspetti e le modalità del sondaggio, che potrà essere fornita anche utilizzando un modello semplificato di informativa predisposta dal Garante.

La PA su Internet: le regole del garante per rispettare la privacy dei cittadini e dei dipendenti

Il Garante per la protezione dei dati personali ha fissato le regole in base alle quali le pubbliche amministrazioni possono diffondere on line atti e documenti amministrativi contenenti dati personali senza ledere la riservatezza di cittadini e dipendenti e rispettare i principi stabiliti dalla normativa sulla privacy.

Le linee guida varate dal Garante definiscono infatti un primo quadro unitario di misure e accorgimenti che la P.a. deve adottare sia nel caso che la pubblicazione on line sia effettuata a fini di trasparenza dell'attività amministrativa, di pubblicità degli atti o di consultazione da parte di singoli soggetti.

Queste in sintesi le principali indicazioni contenute nelle Linee guida:

- Le amministrazioni pubbliche possono mettere in rete atti o documenti contenenti dati personali solo sulla base di una norma di legge e di regolamento che lo preveda e devono rispettare i principi di necessità, proporzionalità e pertinenza. Rimane fermo il generale divieto di diffondere dati sulla salute.

- La reperibilità dei documenti deve essere assicurata attraverso motori di ricerca interni al sito, limitando l'indicizzazione dei documenti da parte dei motori di ricerca esterni.

- I dati devono comunque rimanere disponibili soltanto per il tempo previsto dalle norme di settore. In mancanza di queste, le pubbliche amministrazioni devono individuare congrui limiti temporali oltre i quali i documenti devono essere rimossi.

- Contro i rischi di riproduzione e riutilizzo dei file contenenti dati personali, devono essere installati software e sistemi di alert che consentono di riconoscere e segnalare accessi anomali al fine di mettere in atto adeguate contromisure.

Relazione 2011 del Garante Privacy

In data 23 Giugno 2011 ha presentato presso la sala della Lupa la relazione sul 14° anno di attività dell'Autorità e sullo stato di attuazione della normativa privacy.

Questi alcuni dei principali e complessi ambiti nei quali il Garante ha assicurato il suo intervento nel corso del 2010 a difesa dei singoli individui e della collettività:

- telefonate pubblicitarie indesiderate;
- internet e le nuove tecnologie cloud computing;
- sistemi di videosorveglianza;
- social network;
- la trasparenza on line della pubblica amministrazione;

Interventi rafforzati dai maggiori poteri sanzionatori ora a disposizione dell'Autorità.
Le ispezioni effettuate nel 2010 sono state circa 500 e i controlli hanno riguardato numerosi settori, in particolare:

- gli operatori telefonici;
- le strutture sanitarie pubbliche e private;
- i sistemi di videosorveglianza;
- il sistema della fiscalità;
- le società di marketing;
- gli istituti di credito;

Le violazioni amministrative contestate, compreso il primo semestre 2011, sono state oltre 500, con un ammontare di circa 4 milioni di euro le sanzioni amministrative già riscosse.
Non meno rilevante l'attività del Garante a livello internazionale, infatti i Garanti europei si sono occupati

- dei nuovi servizi offerti da Google;
- delle direttive del "pacchetto telecom" che introducono nuove regole all'uso dei cookies ed al tracciamento degli utenti;
- i sistemi di videosorveglianza;
- delle tecniche di profilazione legate alla alla "pubblicità comportamentale";
- della riforma della direttiva UE sulla privacy;
- delle "regole vincolanti di impresa" per il trasferimento dati all'interno delle multinazionali.

Il Garante ha inoltre contribuito ai lavori dei gruppi che, in sede OCSE e presso il consiglio d'Europa, si occupano della protezione dei dati.
E' stato inoltre riconfermato per il quinto anno consecutivo la presidenza del Garante italiano all'interno dell'Autorità garanti europea.

Banche: clienti più sicuri con il tracciamento delle operazioni

Il garante privacy ha fissato delle regole alle quali dovranno attenersi banche e Poste Italiane spa, relativamente all'attività bancaria e finanziaria, per "blindare" il sistema informativo e garantire un corretto trattamento dei dati dei correntisti.
Vista l'assenza di una normativa che obbliga le banche a tracciare tutte le operazioni l'Autorità garante ha ritenuto di prescrivere agli istituti bancari l'adozione di rigorose misure.

- Ogni operazione di accesso ai dati dei clienti, sia che comporti movimentazione di denaro o sia una semplice consultazione, dovrà essere tracciata attraverso una serie di elementi:
  - la data e l'ora di esecuzione
  - il codice della postazione di lavoro utilizzata
  - il codice del cliente ed il tipo di rapporto contrattuale "consultato" (numero del conto corrente, fido, mutuo, deposito titoli)

  In questo modo la banca saprà sempre quando e chi ha avuto accesso ad un determinato conto corrente o ha effettuato operazioni.
  Questi file di log di tracciamento delle operazioni, comprese quelle di semplice consultazione, dovranno essere conservati per un periodo di almeno 24 mesi.

- Le banche, dovranno prevedere l'attivazione di alert che individuano comportamenti anomali o a rischio (es. consultazione massive o accessi ripetuti su uno stesso nominativo)

Foto: juan-duque.blogspot.com

- Almeno una volta l'anno la gestione dei dati bancari dovrà essere oggetto di un'attività di controllo interno da parte degli istituti, per verificare la rispondenza alle misure organizzative, tecniche e di sicurezza previste dalla normativa vigente.
  Detto controllo, che dovrà essere adeguatamente documentato, dovrà essere eseguito da personale diverso da quello che ha accesso ai dati dei clienti.
  Inoltre le verifiche sulla legittimità e liceità degli accessi, sull'integrità dei dati e delle procedure informatiche dovranno essere effettuate anche a posteriori, sia a campione che a seguito di allarme.

- Le banche sono inoltre tenute a comunicare al cliente eventuali accessi non autorizzati al proprio conto e di rendere note al Garante eventuali violazioni di particolare rilevanza (per quantità, qualità dei dati, numero dei clienti)

Proroga al provvedimento del 24 febbraio 2011 per gli operatori telefonici

Il Garante ha concesso una proroga, al 12 Settembre 2011, a tutti gli operatori telefonici di adottare le misure e gli accorgimenti indicati nel provvedimento del 24 Febbraio 2011 recante "Modelli" di informativa e di richiesta di consenso al trattamento dei dati personali relativi agli abbonati, ai servizi di telefonia fissa e mobile.

Videosorveglianza e tutela aziendale

A una società che opera nel settore della componentistica elettronica è stato consentito di conservare per novanta giorni le immagini registrate mediante l'impianto di videosorveglianza.

Lo ha stabilito l'Autorità Garante per la protezione dei dati personali che ha accolto l'istanza di verifica preliminare, presentata dalla medesima società al fine di rafforzare i propri standard di sicurezza.

La società richiedente si avvale di un sistema di videosorveglianza costituito da 18 telecamere, debitamente segnalate prima del raggio di azione dei dispositivi, ed era stata autorizzata dalla Direzione provinciale del lavoro a conservare le immagini registrate per un tempo non superiore ai due giorni.

L'ubicazione isolata del sito, il delicato settore produttivo in cui l'azienda opera e la peculiare attenzione posta a livello sia nazionale che internazionale rispetto alla fissazione comune di elevati parametri di sicurezza nel settore elettronico e informatico, giustificano - a parere del Garante - il prolungamento fino a novanta giorni della conservazione delle sole immagini relative a eventi che generano allarme (incidenti, porte di uscita emergenza aperte, porte e finestre forzate, allarme sensori sui vetri ecc.).

I filmati registrati su postazioni dedicate e conservati nei locali server con sistema a doppia password, saranno consultabili solo su specifica richiesta delle autorità inquirenti.

Enti caritativi e "carta acquisti": ok del Garante alla sperimentazione

L'Autorità ha espresso parere favorevole sullo schema di decreto del Ministro del Lavoro e delle politiche sociali, recante norme che consentono agli enti caritativi di partecipare, in via sperimentale, alla gestione del programma "carta acquisti".

In base alle nuove norme, i Ministeri del lavoro e delle politiche sociali e dell'economia e delle finanze - titolari del trattamento dei dati per la social card - devono nominare responsabili del trattamento sia l'Inps ("Soggetto attuatore" del programma sperimentale), sia i comuni e gli enti caritativi coinvolti.
Sarà compito degli enti caritativi individuare un elenco delle "persone in condizioni di maggiore bisogno".

I dati personali dovranno essere trattati in base al principio di pertinenza, non eccedenza e, in caso di dati sensibili, anche di indispensabilità.

Il Garante per la privacy, pur valutando positivamente l'attuale testo, si è comunque riservato di esprimere un ulteriore parere sullo specifico provvedimento dell'Inps che dovrà individuare le misure di sicurezza da adottare per il trattamento dei dati personali. L'Autorità infine verificherà il contenuto dei questionari che il Ministero del lavoro predisporrà al fine di valutare gli effetti della sperimentazione.

Foto: ilsole24ore.com

Redditi online: contrario alla pubblicazione delle dichiarazioni il Garante della Privacy

Un deciso no alla pubblicazione su Internet delle dichiarazioni dei redditi dei cittadini italiani arriva dal Garante della Privacy. Si tratta di "materiale terribilmente pericoloso" che andrebbe a ledere il diritto alla riservatezza.

Il rischio che si corre? L'odio sociale. Si esprime con questi termini il Garante della Privacy, Francesco Pizzetti, in merito alla proposta di pubblicare online le dichiarazioni dei redditi dei cittadini italiani.

Secondo quanto previsto dalla rivisitazione della manovra finanziaria, dovranno essere le amministrazioni comunali a mettere sul web i dati comunicati dall'Agenzia delle Entrate.

Ma il Garante invita alla cautela. Intervistato dal quotidiano La Repubblica spiega che si tratta di "materiale terribilmente pericoloso" e che, come è successo nel 2008 quando un analogo provvedimento è stato adottato dall'ex ministro dell'Economia Vincenzo Visco, può provocare un "odio sociale" che oltrepasserebbe "i limiti e gli obiettivi della nuova norma se mai dovesse essere approvata".

Accanto alla pubblicazione del reddito, ci sono altre informazioni personali, come la scelta dell'ente a cui devolvere l'8 per mille o le eventuali esenzioni delle spese sanitarie, che potrebbe diventare pubbliche violando inevitabilmente il diritto alla riservatezza.

Foto: repubblica.it

Sono due le speranze dichiarate di Pizzetti. La prima è di "grande attenzione e senso di responsabilità nel passare dall'attuale sistema di consultazione sul cartaceo, con paletti ben definiti, a quello online dove i dati una volta pubblicati difficilmente sono cancellabili". La seconda fa riferimento agli aspetti procedurali: "Mi aspetto che l'Autorità sia sentita dal legislatore prima di procedere per definire modalità e criteri".

Senza l'informativa privacy sul sito scatta la multa

Da una serie di controlli effettuati dal Nucleo Privacy della Guardia di Finanza, sono numerose le aziende che si sono viste infliggere salatissime multe per omessa o inidonea informativa sul proprio sito web. La leggerezza di mettere un bel sito online senza preoccuparsi delle incombenze sulla normativa del trattamento di dati personali, può davvero costar caro.

E non sono pochi quelli che più o meno coscientemente ignorano l'obbligo di informativa dovuto all'interessato quando si raccolgono dati personali sul web, siano essi giusto il nome e cognome, o un banale numero di telefono. Basta prendersi qualche minuto per navigare in internet digitando su Google parole chiave tipo "form contatto" o simil e curiosare tra i risultati per rendersi conto quante siano le imprese (anche note o operanti in settori sensibili!) che alla bella vista di tutti si rendono passibili di multe da capogiro pubblicando specifici form che il visitatore può compilare con i propri dati senza essere benché minimamente informato circa l'uso dei suoi dati personali. A volte è richiesto il solo consenso, che dovrebbe essere espresso dopo lettura della privacy policy, e infatti ciò non basta ad evitare la multa, che punisce l'omissione dell'informativa. Senza pensare che, proprio perché la rete diffonde tutto a tutti, omettere di provvedere l'informativa ai sensi dell'art.13 del Dlgs 196/2003, espone l'ingenuo imprenditore a vendette di concorrenti spietati, acerrimi nemici, o semplici invidiosi, i quali non potrebbero trovarsi in mano arma migliore per fare un dispetto che potrà avere effetti devastanti. Considerando quindi la delicatezza delle questioni legate all'adempimento obbligatorio dell'informativa, e le segnalazioni che ci pervengono circa le multe comminate, riteniamo opportuno rammentare che il quadro sanzionatorio è diventato particolarmente pesante dopo il Dlgs n. 207/2008,che ha innalzato notevolmente le sanzioni edittali. Non a caso molti preferiscono definire spontaneamente le contestazioni mediante l'oblazione in via breve o mediante ordinanza. Il Dlgs n. 207/2008, infatti, come spiegava la relazione sull'attività del garante per il 2009, ha comportato: un aumento delle pene pecuniarie previste per ciascuna violazione; la previsione di nuove ipotesi sanzionatorie; la creazione di meccanismi per consentire una maggiore modulabilità della sanzione in rapporto al caso concreto in ragione della minore o maggiore gravità, della circostanza che le violazioni siano state commesse in relazione a banche di dati di particolare rilevanza o dimensioni, del coinvolgimento di un maggior numero di interessati e delle condizioni economiche del contravventore. Nello specifico caso della violazione dell'art.13 per omessa o inidonea informativa, si applicano le previsioni dell'art.161 del Dlgs 196/2003 che comportano sanzioni da 6.000 a 36.000 euro.

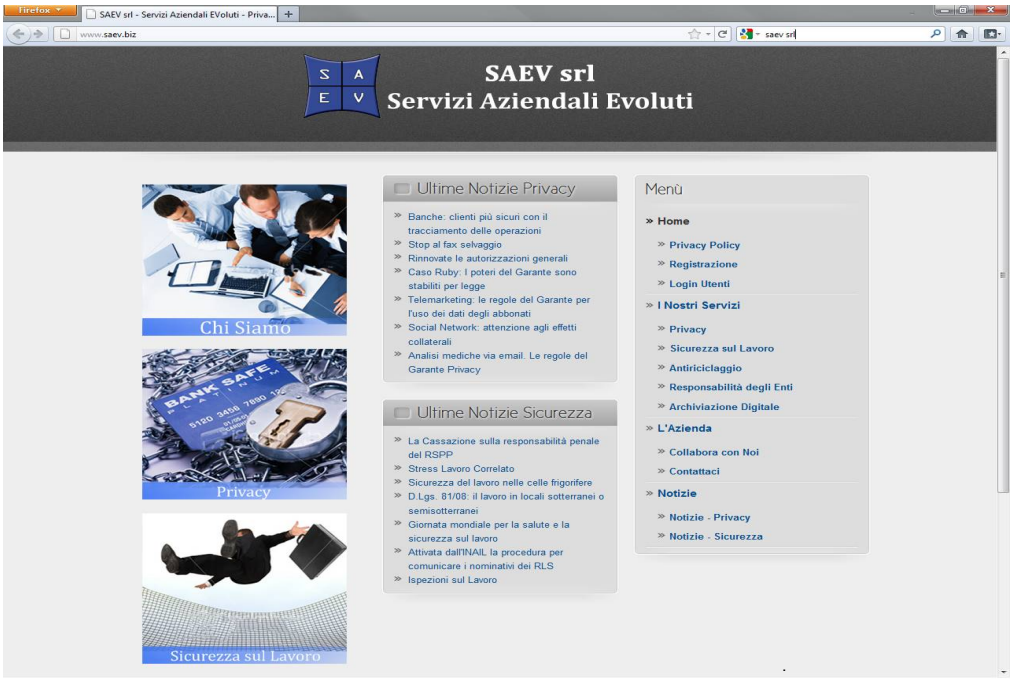


Foto: Sito Saev - www.saev.biz

La multa può essere annullata se il comune non redige il Dps

Con una sentenza del Giudice di Pace di Bari, un automobilista ha chiesto ed ottenuto l'annullamento di una multa presa per un semaforo rosso additando la mancata redazione del documento programmatico sulla sicurezza dei dati personali da parte del Comune che aveva comminato la sanzione.
Nel ricorso presentato, il cittadino ha infatti invocato l'art. 11 comma 2 del Dlgs 196/2003, il quale prescrive che "i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati", denunciando allo stesso tempo il fatto che il Comune non aveva adottato le misure di sicurezza per una adeguata protezione dei dati personali, né tantomeno redatto il Dps, obbligatorio per tutti quei soggetti che trattano dati personali di carattere sensibile con strumenti elettronici, (oltre a quelli dei propri dipendenti), come appunto un qualsiasi comune d'Italia, che generalmente gestisce quotidianamente dati "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" del cittadino.

Il Comune, da parte sua, non ha "in alcun modo provato il rispetto delle regole basilari né ha saputo dimostrare il contrario", e questo ha subito convinto il giudice pugliese ad accogliere il ricorso annullando la sanzione di 150 euro e la relativa decurtazione di 6 punti, condannando inoltre la pubblica amministrazione alla rifusione delle spese e competenze di causa quantificate in 180,00 euro.

Foto: Autoblog.it

Ispezioni Privacy utenti Entratel

L'agenzia delle Entrate ha comunicato che a partire dal secondo semestre 2011 inizieranno nuovi e più serrati controlli sul rispetto della normativa privacy, in particolare sul rispetto degli obblighi di riservatezza, per gli incaricati alla trasmissione telematica delle dichiarazioni dei redditi in particolare i CAF e gli intermediari abilitati al servizio Entratel.
Quanto all'esito delle verifiche, per le eventuali omissioni riscontrate rispetto agli obblighi di riservatezza, si rischia la revoca dell'abilitazione al servizio **ENTRATEL.**

In generale, i controlli riguarderanno l'adozione di tutte le misure necessarie a proteggere i dati sensibili che gli intermediari vengono necessariamente a conoscenza per lo svolgimento del proprio lavoro.

I contenuti dei controlli come precisati dall'**Agenzia delle Entrate** riguarderanno: la struttura organizzativa dell'intermediario; le misure di sicurezza adottate in riferimento ai mezzi tecnologici utilizzati, altre misure di sicurezza.

Nell'ambito dei controlli della struttura organizzativa dell'intermediario, rientra anche l'individuazione dei responsabili, anche esterni del trattamento dei dati e la designazione delle persone incaricate del trattamento dei dati e l'ambito di trattamento a loro consentito.

Il controllo è esteso anche all'**esistenza del documento programmatico sulla sicurezza (DPS),** obbligatorio entro il 31 marzo di ogni anno, in relazione all'obbligo generale di protezione dei dati personali, dall'art. 34, comma 1, lett. g) e dal punto 19 dell'allegato B) del Codice della privacy (*contenente il "Disciplinare tecnico in materia di misure minime di sicurezza"*).

Ancora, in vista del controllo, bisognerà stare attenti a una corretta politica di **gestione delle password** che preveda, fra l'altro, l'attribuzione a determinati soggetti del compito di **amministrare le utenze** per l'accesso ai sistemi informatici e l'adozione di misure per mantenere riservate le informazioni che consentono l'accesso ai servizi telematici del **Codice della privacy** e art. 5, comma 6, del provv. 10 giugno 2009.

Cloud computing: indicazioni per l'utilizzo consapevole dei servizi

Foto: repubblica.it

Il cloud computing non è un fenomeno temporaneo o una moda, ma il passo successivo dell'evoluzione nel modo in cui si utilizza la Rete Internet, che da strumento per la sola condivisione documentale, diviene porta d'accesso alle risorse elaborative di un provider di servizi.

Il cloud computing, o nuvole informatiche, è un insieme di modelli di servizio che si sta diffondendo con grande rapidità tra imprese, pubbliche amministrazioni e cittadini perchè incoraggia un utilizzo flessibile delle proprie risorse o di quelle messe a disposizione da un fornitore di servizi specializzato.
Nell'ambito del cloud computing è possibile distinguere tra **private cloud e public cloud.**

Una **private cloud** o nuvola privata, organizzazione, nei confronti del quale il titolare dei dati può spesso esercitare un controllo puntuale. Le private cloud possono essere paragonate ai tradizionali "data center"

Nel caso delle public cloud o nuvola pubblica, l'infrastruttura è di proprietà di un fornitore specializzato nell'erogazione di servizi che mette a disposizione i propri sistemi attraverso l'erogazione via web di applicazioni informatiche, di capacità elaborativa e di stoccaggio.

La fruizione di tali servizi avviene tramite la rete Internet e implica il trasferimento dell'elaborazione o dei soli dati presso i sistemi del fornitore del servizio, il quale assume un ruolo importante in ordine all'efficacia delle misure adottate per garantire la protezione dei dati che gli sono stati affidati.

Sul mercato, a seconda delle esigenze dell'utente, sono disponibili varie soluzioni di cloud computing erogate secondo modalità che ricadono in linea di massima in tre categorie, dette "modelli di servizio":

Cloud Infrastructure as a Service

Infrastruttura Cloud resa disponibile come servizio;
Il fornitore noleggia un'infrastruttura, cioé server virtuali remoti che l'utente finale può utilizzare con tecniche e modalità che ne rendono semplice, efficace e produttiva la sostituzione o l'affiancamento ai sistemi già presenti nei locali dell'azienda.

Cloud Software as a Service

Software erogato come servizio cloud; il fornitore eroga via web una serie di servizi applicativi ponendoli a disposizione degli utenti finali. Tali servizi sono spesso offerti in sostituzione delle tradizionali applicazioni installate localmente dall'utente sui propri sistemi (fogli di calcolo, elaborazione di testi, la rubrica e i calendari, la posta elettronica).

Cloud Platform as a Service

Piattaforme software fornite via web come servizio; il fornitore offre soluzioni per lo sviluppo e l'hosting evoluto di applicazioni. In genere questo servizio è rivolto a operatori di mercato che li utilizzano per sviluppare e ospitare soluzioni applicative proprie. Il servizio erogato dal fornitore elimina la necessità per il fruitore di doversi dotare internamente di strumenti hardware o software specifici o aggiuntivi.

Tuttavia, è bene evidenziare come l'adozione di servizi esternalizzati non esime le imprese e le amministrazioni pubbliche dalle responsabilità che vengono loro attribuite, in particolare, dalla disciplina in materia di protezione dei dati personali.

I trattamenti di dati personali richiedono, infatti, sempre un'attenta ponderazione dei rischi legati alla sicurezza e alla fruibilità di informazioni, indipendentemente dalle modalità di trattamento.

Prima di adottare un sistema basato nel cloud computing è necessario valutare attentamente il rapporto tra rischi e benefici, minimizzando i primi attraverso una attenta verifica dell'affidabilità del fornitore di servizi al quale ci si intende affidare, in particolare bisogna:

Effettuare una verifica in ordine all'affidabilità del fornitore

Gli utenti dovrebbero accertare l'affidabilità del fornitore e le garanzie offerte in ordine alla confidenzialità dei dati e alle misure adottate per garantire la continuità operativa a fronte di eventuali malfunzionamenti. Gli utenti dovrebbero valutare le caratteristiche qualitative dei servizi di connettività di cui si avvale il fornitore in termini di capacità e affidabilità. Ulteriori criteri in base ai quali è possibile valutare l'affidabilità di un fornitore emergono dall'impiego di personale qualificato, dall'adeguatezza delle infrastrutture informatiche e di comunicazione, dalla disponibilità ad assumersi responsabilità, esplicitamente previste dal contratto di servizio, derivanti da eventuali falle nel sistema di sicurezza o a seguito di interruzioni del servizio.

Ponderare prioritariamente rischi e benefici dei servizi offerti

Prima di optare per l'adozione di servizi di cloud computing è opportuno che l'utente verifichi la quantità e la tipologia di dati che intende esternalizzare. Tale analisi valutativa dovrà evidenziare l'opportunità o meno di ricorrere a tali servizi, limitandone l'uso ad esempio in presenza di dati sensibili, nonché l'impatto che l'utente può avere in termini economici e organizzativi nel caso in cui si verifichi l'indisponibilità di tali dati, pur se parziale o per periodi limitati, o peggio la loro perdita o cancellazione.

Privilegiare i servizi che favoriscono la portabilità dei dati

E' consigliabile ricorrere a servizi di cloud computing che facilitino la transizione da un sistema cloud ad un altro, anche se gestiti da fornitori diversi.

Verificare le politiche di persistenza dei dati legate alla loro conservazione

In fase di acquisizione del servizio cloud è opportuno approfondire le politiche adottate dal fornitore relative ai tempi di persistenza dei dati nella nuvola. Da una parte l'utente dovrebbe accertare il termine ultimo, oltre il quale il fornitore cancella definitivamente i dati che gli sono stati affidati. Dall'altra il fornitore dovrà presentare adeguate garanzie, assicurando che i dati non saranno conservati oltre i suddetti termini o comunque al di fuori di quanto esplicitamente stabilito con l'utente stesso. In ogni caso, i dati dovranno essere conservati nel rispetto delle finalità e delle modalità concordate, escludendo duplicazioni e comunicazioni a terzi.

Informarsi su dove risiederanno concretamente i dati

Sapere in quale Stato risiedono fisicamente i server sui quali vengono allocati i dati, è determinante per stabilire la giurisdizione e la legge applicabile nel caso di controversie tra l'utente e il fornitore del servizio. L'utente, prima di inserire i dati nella nuvola informatica, dovrebbe assicurarsi che il trasferimento tra i diversi paesi in cui risiedono le cloud avvenga nel rispetto delle cautele previste a livello di Unione Europea in materia di protezione di dati personali, che esigono particolari garanzie in ordine all'adeguatezza del livello di tutela previsto dagli ordinamenti nazionali per tale tipo di informazioni.

Assicurarsi la disponibilità dei dati in caso di necessità

Nell'utilizzo dei servizi di cloud computing, si raccomanda di mantenere una copia di quei dati dalla cui perdita o indisponibilità potrebbero conseguire danni economici, per l'immagine o in generale relativi alla missione e alle finalità perseguite dall'utente.

Attenzione alle clausole contrattuali

Una corretta e oculata gestione contrattuale può supportare sia l'utente, sia il fornitore nella definizione delle modalità operative e dei parametri di valutazione del servizio, oltre a individuare i parametri di sicurezza necessari per la tipologia di attività gestita. É infatti importante valutare gli obblighi e le responsabilità in caso di perdita, smarrimento dei dati custoditi nella nuvola e le conseguenze in caso di decisione di passaggio ad altro fornitore. Costituiscono elementi da privilegiare la previsione di garanzie di qualità chiare, corredati da penali che pongano a carico del fornitore eventuali inadempienze o le conseguenze di determinati eventi (ad es. accesso non consentito, perdita dei dati, ecc..)

Non perdere di vista i dati

E' sempre opportuno che l'utente valuti accuratamente il tipo di servizio offerto dal fornitore verificando sei i dati rimarranno nella sua disponibilità fisica, oppure se questo svolga un ruolo da intermediario, ovvero offra un servizio progettato sulla base delle tecnologie messe a disposizione da un operatore terzo.

Formare adeguatamente il personale

Il personale preposto al trattamento dei dati attraverso i servizi cloud computing dovrebbe essere sottoposto a specifici interventi formativi, che evidenziano adeguatamente le modalità più idonee per l'acquisizione e l'inserimento dei dati nella cloud, la consultazione e in generale l'utilizzo allo scopo di mitigare i rischi per la protezione dei dati derivanti non solo da eventuali comportamenti sleali o fraudolenti, ma anche causati da errori materiali, leggerezza o negligenza, circostanze che potrebbero dare luogo ad accessi illeciti, perdita di dati o trattamenti non consentiti.

Esigere e adottare opportune cautele per tutelare la confidenzialità dei dati

Nell'ottica di proteggere la confidenzialità dei propri dati, l'utente dovrebbe valutare anche le misure di sicurezza utilizzate dal fornitore. In generale si raccomanda di privilegiare i fornitori che utilizzano a tal fine tecniche di trasmissione sicure, tramite connessioni cifrate, coadiuvate da meccanismi di identificazione dei soggetti autorizzati all'accesso, la cui complessità sia commisurata alla criticità degli stessi. Nella maggior parte dei casi risulta adeguato l'utilizzo di semplici meccanismi di identificazione, basati su username e password. Nell'ipotesi in cui il trattamento riguardi particolari tipologie di dati, quali sanitari, genetici, reddituali e biometrici, si raccomanda anche la conservazione in forma cifrata.

Nelle emittenti private imperversa lo spot "Spia chi vuoi, basta un sms", ma se non è un inganno allora è reato

Il messaggio dello spot televisivo è semplice e diretto: basta inviare il numero di telefono che intendi controllare e per cinque euro a settimana potrai leggere tutti gli sms in entrata e in uscita da quell'utenza. La pubblicità, che sta passando su alcune importanti emittenti private di caratura nazionale, punta dritto alla paura primordiale del tradimento e pretende di fornire uno strumento hi-tech per il controllo del proprio partner.

Con la sola conseguenza, per ora, di aver provocato sul web un vespaio di polemiche. Anche perché è tecnicamente impossibile accedere ai messaggi se non si istalla un software sul telefonino da spiare. Come fa notare Francesco Pizzetti, alla guida del Garante per la protezione dei dati personali (meglio noto come Garante della Privacy): "Se nello spot che sta provocando tante polemiche sui blog si promette davvero di svelare i messaggi di qualcun altro, siamo davanti ad una pubblicità ingannevole. Già in passato abbiamo condotto indagini su programmi simili, arrivando alla conclusione che non è possibile ottenere i risultati promessi". Insomma, queste magie non funzionano, eppure c'è chi le propone ciclicamente dal 2006. Ma se il servizio funzionasse davvero, lo spot allora istigherebbe ad infrangere l'articolo 615bis del codice penale sulle interferenze illecite nella vita privata. Reato per il quale è prevista una pena che va dai sei mesi ai quattro anni di reclusione.

L'uso di software professionali che, attraverso l'istallazione di un programma sul cellulare preso di mira, consentono sul serio di vagliare gli sms altrui, attivare il microfono senza che il proprietario del cellulare se ne accorga o avere l'elenco delle telefonate fatte e ricevute, è illegale.
Di recente ne è stato lanciato uno per iPhone con molte meno pretese, SpyCell, che proponeva di "localizzare chiunque tramite il numero di telefonino". Anche in questo caso si è rivelata una promessa vuota, tant'è che le recensioni sono impietose. Alla fine della descrizione, sull'App Store, si legge però una cosa interessante: "Il software è a solo scopo interattivo in quanto è illegale localizzare un cellulare altrui (e praticamente impossibile)".

Come dire: abbiamo scherzato e se ci siete cascati, dandoci dei soldi, il problema è vostro.
In attesa che l'Agcom, l'Autorità per le garanzie nelle comunicazioni, intervenga su segnalazione dell'Antitrust (Garante della concorrenza), la pubblicità del servizio per spiare gli sms continua ad andare in onda. In frangenti simili solo l'Antitrust può e deve chiedere un parere alla prima, la quale lo emette in circa 30 giorni. In questo caso l'Agcom ha preferito non rivelare se è stata o meno contatta a riguardo.

Arriva Tdl-4, la balena bianca del cybercrime che ha infettato 4,5 milioni di computer

È l'ultima balena bianca del crimine su internet, invisibile e capillare: la rete Tdl-4 ha infettato almeno 4,5 milioni di computer nel mondo e il 3% in Italia. Non causa danni alla normale attività degli utenti, ma apre varchi per inviare spam, pubblicità e software malevoli, utilizzabili per truffe.

E' come aprire una rete di autostrade su internet in grado di veicolare dati nei computer colpiti, senza che nessuno se ne accorga. E può attaccare anche i sistemi operativi come Windows 7.

Secondo gli analisti la Tdl-4 è praticamente indistruttibile, in quanto i pirati informati la hanno progettata per evitare che sia annientata.

Può connettersi con una rete per la condivisione di file, Kad network, impiegata per inviare su eMule video e musica: in questo modo diventa gestibile a distanza attraverso un canale sicuro di cybercriminali.

Le comunicazioni avvengono con pacchetti di dati cifrati tanto che ai software antivirus diventano invisibili, attivandosi prima dell'avvio del sistema operativo.

Il Web ci guarda: siamo tutti spiati

Le telefonate sono gratis, incluse quelle internazionali o verso i cellulari, se a precederle è un breve spot della nostra marca di scarpe preferita.

Se scriviamo ad un amico che vogliamo visitare una capitale europea, non appena gli inviamo il messaggio, Gmail ci indica dove prenotare i biglietti. Apple e Amazon, ci propongono i libri, i film, gli album e le app che ancora non abbiamo acquistato e, possiamo starne certi, rispecchiano i nostri gusti.

La pubblicità, insomma, ha smesso d'inseguire, di affannarsi a sparare nel buio; riconosce chi ha davanti e sa a menadito che cosa vuole, deve solo ricordarglielo.
A confidarle ogni cosa siamo noi, al ritmo dei clic con il mouse, delle parole digitate sulla tastiera, dei "mi piace" sussurrati ai social network.
Perchè non c'è azione che non venga monitorata, analizzata, sezionata e rivenduta in blocco a scopi promozionali.

E' un gioco di ruolo e di ruoli che ingrassa tutti i colossi della rete: loro offrono decine di servizi cui mai potremmo rinunciare, senza chiedere, in cambio, nemmeno un centesimo; noi alimentiamo un business gigantesco di cui siamo artefici e, destinatari.

Dietro questo gioco immenso ci sono le strategie dei protagonisti di questa partita planetaria.

Google, il segreto sta nella "parola chiave"

La miniera d'oro della propaganda in target sono le cosiddette AdWords: si impostano frasi o parole legate alla propria attività o alla propria azienda e l'annuncio compare come link sponsorizzato quando qualcuno le include in una ricerca.
Così, se confidiamo a un amico che abbiamo voglia di innamorarci, può comparire il collegamento a un sito per cuori solitari; se gli riveliamo di avere paura della prova costume, ecco il link alla nuova rivoluzionaria dieta o alla crema snellente che fa miracoli.
Gli inserzionisti ci mettono l'abilità di annodare aspirazioni e prodotti, Google fornisce uno strumento che le ha riempito le casse.
All'interno di Youtube, c'è il sistema pubblicitario che si chiama Insight.
A comporlo sono tutti gli utenti registrati che guardano un video: agli inserzionisti vengono rivelate in modo aggregate statistiche su età, sesso e paese del pubblico; quali termini di ricerca hanno portato a quel filmato e persino i "punti di interesse", ovverosia in quale preciso punto il video è stato più visto.

Facebook, il "profilo" che diventa un mirino

La geniale intuizione del suo creatore, Mark Zuckerberg, non è stata quella di convincere oltre 500 milioni di persone nel mondo (18 delle quali in Italia) a rinunciare a una grossa fetta di privacy. Il colpo da maestro è stato piuttosto quello di trasformare il social network nella macchina perfetta per le promozioni target. I "profili" degli iscritti fanno gola perchè non sono costruiti da un computer, ma dagli iscritti stessi. E nel vendere gli spazi su Facebook non va tanto per il sottile, usa ogni singolo dettaglio che gli comunichiamo: consente agli inserzionisti d'impostare filtri per fasce d'età, collocazione geografica, preferenze sessuali, tipo di lavoro, interessi e hobby.

Amazon e Apple, l'iTunes store sa tutto di te

La società della mela morsicata è stata fra le prime a sviluppare meccanismi per fotografare i nostri gusti: si è inventata Genius, un sistema che raccoglie le informazioni dalla libreria di iTunes e le invia ad un cervellone che sforna le proposte che fanno a caso nostro, tutte ovviamente pronte per essere acquistate. Simile è la strategia del colosso dell'e-commerce Amazon, che tiene traccia di ricerche e acquisti per suggerire prodotti simili.

Microsoft Skype, tiro al bersaglio ai profili

Quanto a Microsoft, anche l'azienda madre del sistema operativo più diffuso al mondo e della console Xbox ha capito che i profitti non si fanno solo con i videogiochi e i programmi. Perciò propone il "profile targeting", che permette alle aziende di scegliere a quali utenti della chat di Messanger o di Hotmail rivolgersi, scegliendo tra i 167 milioni di iscritti in tutta Europa su Windows Live. Oltre ai filtri classici, si possono impostare l'ora e il giorno in cui si collegano e il metodo di accesso per tipo di connessione e browser. Il vero colpaccio, però, la Microsoft l'ha messo a segno acquistando Skype per 8,5 miliardi di dollari. Così l'azienda ha accesso ai 600 milioni di utenti del marchio leader delle telefonate in tecnologia Voip.

Morti bianche e invisibili

In occasione della sessantunesima giornata nazionale delle vittime degli incidenti sul lavoro, L'Anmil (Associazione nazionale mutilati e invalidi sul lavoro) ha diffuso i dati sulle morti sul lavoro che nel 2010 ha causato circa 1000 vittime, poco meno di tre al giorno.

Morti che non fanno notizia se non quando le vittime sono molte: in un paesino della Val di Non un trattore ha investito quattro operaie impegnate nella raccolta delle mele, una è morta sul colpo, le altre tre sono ferite, una in fin di vita, a Barletta la settimana scorsa crolla una palazzina e muiono cinque donne, a Molfetta cinque operai morirono per le esalazioni di zolfo nell'autocisterna dove lavoravano, a Mineo (CT) sei operai morirono nel depuratore o come alla Thyssen-Krupp dove nel 2007 morirono sette operai bruciati vivi.

Qualche anno fa fece scalpore l'esito di uno studio dell'Eurispes che venne presentato con un titolo ad effetto:
« Infortuni sul lavoro, peggio di una guerra ». Dall'aprile del 2003 all'aprile del 2007 i militari della coalizione internazionale che persero la vita furono 3520 mentre dal 2003 al 2006 nel Nostro Paese i morti sul lavoro sono stati 5252, peggio della guerra.

Un fenomeno che il Presidente della Repubblica Giorgio Napolitano ha definito « inacettabile ».

Presidente della Repubblica, Giorgio Napolitano *Foto: Il secolo XIX*

Foto:associazionepmi.it

Per questo, come ha detto, « pur nella crisi economica non può abbassarsi la guardia riducendo gli investimenti nel campo della prevenzione e della sicurezza sul lavoro » Il calo degli infortuni, se di calo si può parlare, tre vittime al giorno, deve essere visto come sottolinea il presidente Napolitano con molta cautela in quanto « il calo degli incidenti è un dato che potrebbe non rispondere alla realtà perchè resta il problema del lavoro nero e dei casi in cui le denunce non vengono fatte ».

La gran parte degli incidenti mortali avviene in settori dove prevalgono informalità e scarsa visibilità. Nell'edilizia: 133 vittime, oltre un quarto del totale, nell'agricoltura: 162 morti, quasi un terzo del totale, dove il maggior numero di vittime è costituito da persone schiacciate dal trattore, che esse stesse guidavano.

Questi dati suggeriscono il motivo della scarsa visibilità attribuita al fenomeno. Gli incidenti e le morti avvengono dietro casa nostra, in campagna, nei cantieri degli edifici in costruzione dove le norme sulla prevenzione e sulla sicurezza sono poco osservate e dove le vittime sono gli stessi imprenditori oppure lavoratori stranieri, i quali, come "vittime", fanno meno notizia di quando sono i responsabili di reati.

Oltre alla perdita di vite umane, che è la cosa più grave e importante, ci sono anche altre cifre allarmanti. L'Anmil ha quantificato la spesa complessiva per gli indennizzi avvenuti sul lavoro che si aggira intorno ai cinque miliardi di euro, senza contare le rendite vitalizie pagate dall'Inail per il 2.500 infortuni al giorno di cui 27 con invalidità permanente e la spesa sanitaria annua per la cura delle vittime di infortunio che è di 3 miliardi e 400 milioni all'anno. Peggio, molto peggio di una guerra.

Quel doloroso "mal di mouse" che tormenta soprattutto le donne

L'uso continuativo del dispositivo del PC è tra le cause principali che provocano la sindrome del tunnel carpale: una patologia sempre più diffusa negli uffici e nelle aziende italiane e di cui soffrono due milioni e 700 mila lavoratrici.

Impossibile al giorno d'oggi pensare di potere fare a meno del computer. Strumento ormai indispensabile nella nostra vita, il pc tuttavia è anche causa di patologie decisamente fastidiose. A partire dalla sindrome da tunnel carpale, la neuropatia dovuta all'irritazione o alla compressione del nervo mediano al polso provocata molto spesso dall'uso intensivo del mouse, talmente diffusa da essere ormai chiamata anche "mal di mouse".

Nel 47% dei casi la neuropatia dipende dal lavoro.
Ovviamente non solo l'utilizzo del mouse provoca questo disturbo: le cause principali sono anche l'uso di utensili non ergonomici o le vibrazioni e le basse temperature. Ma la sindrome da tunnel carpale è sicuramente un fenomeno in netto aumento nella popolazione, in grado di incidere in modo significativo anche da un punto di vista sociale a causa del numero altissimo di giornate lavorative perse: è stato calcolato, infatti, che la sua insorgenza nel 47% dei casi è riconducibile all'attività professionale.

Essenziale una prognosi tempestiva.
Proprio per evitare un così alto disagio è importante la tempestività della prognosi. Decisiva anche una valida ed efficace terapia riabilitativa che permetta di recuperare appieno e in tempi non troppo lunghi la funzionalità dell'arto. Inoltre, una mano priva della sensibilità - tra i principali sintomi della sindrome del tunnel carpale, insieme a formicolii, intorpidimento, gonfiore ma anche dolore e perdita di forza - non ha la stessa funzionalità di una mano con un handicap motorio recuperabile e, di conseguenza, la strategia terapeutica che mira alla ricostruzione della funzione deve dare priorità al recupero sensitivo, senza il quale ogni tentativo di miglioramento motorio sarebbe vano.

Foto: donnamoderna.com

A rischio 2,7 milioni di donne.
Inoltre, si è riscontrato che la patologia colpisce soprattutto le donne e prevalentemente in età adulta: il tasso di incidenza "al femminile" è del 3,4% (contro lo 0,6% per gli uomini), ma si stima che questa neuropatia sia presente in un ulteriore 5,8% di donne non diagnosticato, fino ad arrivare a un picco del 9,2%. Questo vuol dire che in Italia, potenzialmente, si potrebbero ammalare di questa sindrome 2,7 milioni di lavoratrici.

Il mestiere del RLS (Rappresentante dei Lavoratori per la Sicurezza)

Per gli RLS è necessario:

- favorire le proprie competenze attraverso la lettura di leggi, linee guida, conoscendo i diritti e i doveri o attraverso la conoscenza di dati e esperienze di natura tecnica;
- affinare le proprie capacità e abilità comunicative, relazionali, contrattuali, di organizzazione

Una tappa fondamentale del lavoro del RLS è **la riunione periodica di prevenzione,** come indicata dall'art.35 del Decreto Legislativo 81/2008, come elemento del processo di comprensione e gestione del rischio occupazionale e del sistema d'impresa nel suo complesso. I componenti che devono essere presenti **obbligatoriamente** alla riunione sono: il datore di lavoro o un suo rappresentante, l'RSPP, il medico competente se nominato e l'RLS.
I componenti che possono essere presenti **facoltativamente** alla riunione sono: ASPP (Addetti al Servizio di Prevenzione e Protezione), i dirigenti aziendali (seppur non membri del Servizio di Prevenzione Protezione), i consulenti aziendali "esterni" (il cui ruolo è di sostegno tecnico al datore di lavoro), il Servizio di Prevenzione e Sicurezza negli Ambienti di Lavoro della ASL/ASUR.
Detti componenti possono essere presenti a singoli riunioni dietro invito in relazione a temi specifici.
Nel corso della riunione devono essere necessariamente trattati diversi argomenti:

- resoconto delle evoluzioni significative che sono intervenute nel sistema aziendale
- resoconto aggiornato della valutazione dei rischi
- consuntivo degli interventi già realizzati (in ordine alla prevenzione, protezione, promozione della salute e della sicurezza)
- risultati della sorveglianza sanitaria
- analisi degli eventi negativi accaduti
- definizione del programma delle cose che si intende fare

e facoltativamente:

- il dettaglio applicativo del DVR nelle sue varie articolazioni (compreso il DUVRI), specificando già in tale sede "chi fa cosa", con quale grado di responsabilità e autonomia, con quali scadenze temporali per le varie sotto-fasi di processo e con quali risorse.

Una riunione periodica di prevenzione significativa può portare ad un aggiornamento significativo del documento di valutazione dei rischi (DVR) ed eventualmente anche del documento di valutazione dei rischi da interferenza (DUVRI).
Tale aggiornamento può avvenire con un verbale della riunione ben fatto.

La riunione periodica di prevenzione:

- deve essere fatta almeno una volta l'anno anche se non ci sono novità;
- deve avere un "Ordine del Giorno" comunicato per tempo a tutti gli invitati, che comprenda anche la possibilità di inserire "varie ed eventuali";
- deve portare a decisioni, con una chiara definizione degli impegni (anche economici), degli incarichi e delle responsabilità, dei risultati attesi, della scala delle priorità e dei tempi di attuazione;

Della Riunione periodica di prevenzione:

- deve essere redatto un apposito un apposito verbale.

L'RLS in occasione della riunione deve aggiornare la propria conoscenza di tutti i luoghi di lavoro, ascoltare i lavoratori e definire con loro le loro esigenze, gli obiettivi, le priorità, gli strumenti e la scaletta dei tempi anche attraverso l'uso di questionari così da poter confrontare le risposte date dai lavoratori oggi con quelle date qualche tempo prima, per verificare se vi sia la percezione di una stabilità, di un miglioramento o di un peggioramento dello stato di salute soggettivo e della sicurezza.

Alcune delle nostre referenze

- **COAL SOC. COP. ARL.** - Rete di supermercati e distribuzione alimentare
- **GRUPPO FILENI** - distribuzione alimentare
- **MOVIMAC SRL** - vendita, assistenza tecnica e noleggio di carrelli elevatori
- **A.N.P.AS. NAZIONALE E LE PUBBLICHE ASSISTENZE SUL TERRITORIO: CROCE VERDE, CROCE AZZURRA, CROCE BIANCA, CROCE GIALLA**
- **OIKOS** - Centro di Solidarietà ONLUS
- **FONDAZIONE TEATRO DELLE MUSE**

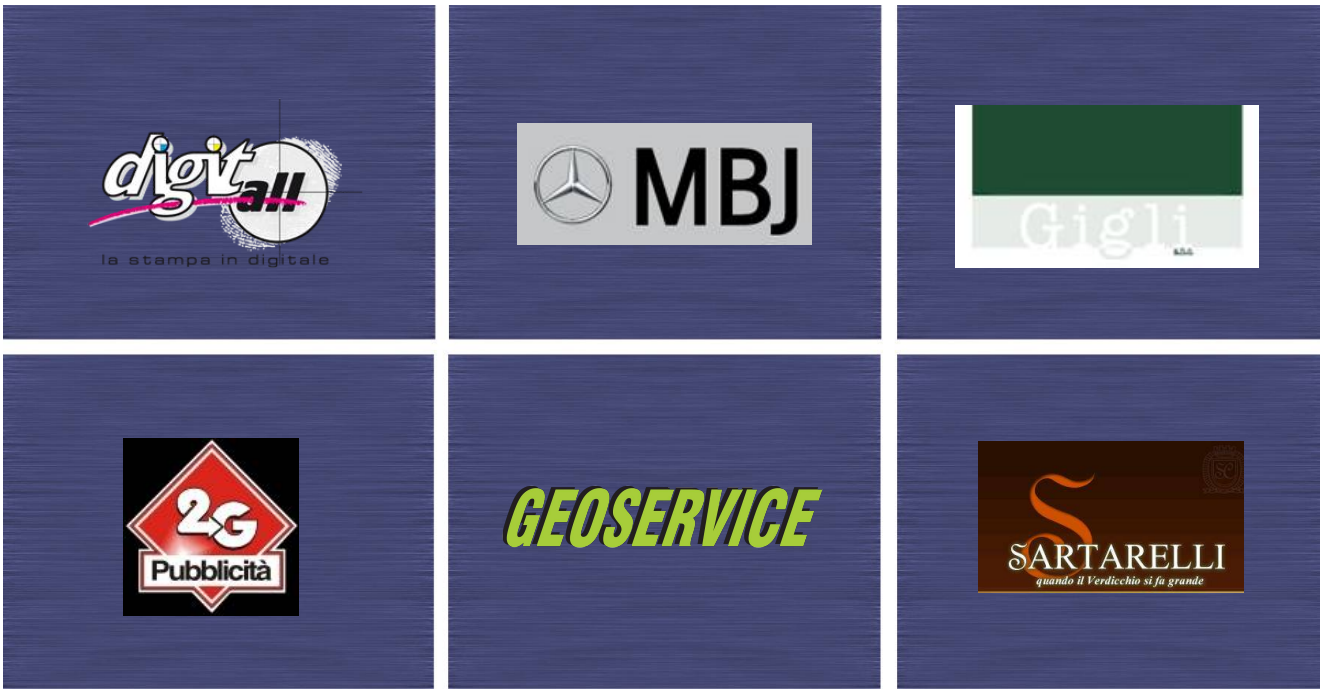
Alcune delle nostre referenze

- **FONDAZIONE CASSA DI RISPARMIO DI JESI (BANCA MARCHE)**
- **INNOFIT** - prodotti elettromedicali, per la cura e il benessere della persona
- **LEONARDI S.P.A.**
- **GRUPPO FITIST** - vigilanza, scorta valori, portierato guardiania, reception, contazione
- **MAIT S.P.A.** - attrezzature per palificazioni
- **FONDAZIONE TEATRO STABILE DELLE MARCHE**
- **GOMMUS SOC.COP. P.A.**

Alcune delle nostre referenze

- **KERATON** - Allevamento monti del Keraton
- **A.N.A.C.I.** - Associazione Nazionale Amministratori Condominiali e Immobiliari
- **AUTOSCUOLA CORINALDESI** - Autoscuola
- **STAMPA NOVA** – Azienda Grafica
- **FONDAZIONE SALESI** - Onlus
- **CASTELVECCHIO** - Cooperativa sociale

Alcune delle nostre referenze



- **DIGITALL** - Stampa digitale
- **AUTOFFICINA MBJ** - Autofficina MBJ Mercedes-Benz
- **GIGLI INFISSI** - Infissi e strutture metalliche
- **2G PUBBLICITÀ** - Pubblicità e comunicazione
- **GEOSERVICE** - Centro Servizi per geometri professionisti della provincia di Ancona
- **SARTARELLI** - Azienda Agricola

… e circa altre 1200 Aziende in italia che hanno scelto i servizi della Saev

I corsi previsti dalla normativa di seguito elencati, per i quali viene rilasciato un attestato sono disponibili anche in dvd.

- **Corsi Antincendio**
- **Corso Prontosoccorso**
- **Corsi di Responsabili RSPP**
- **Corsi Specialistici (es. carrellisti)**

La SAEV organizza la formazione prevista dal punto 19.7 allegato B al D.L.gs 196/03 disponibile anche in DVD e rilascia attestati di partecipazione agli incaricati.

Per conoscere le date dei corsi potete rivolgervi direttamente ai nostri uffici contattando lo 0731/215639

Modulo di iscrizione ai nostri corsi

Se desiderate iscrivervi ai corsi organizzati dalla Saev, compilate il presente modulo ed inviatelo via fax allo 0731 205562 o per e-mail all'indirizzo saev@saev.biz

Qualora vogliate ulteriori informazioni in merito ai nostri servizi potete contattarci ai seguenti recapiti:

- Telefono:0731- 215639
- Fax: 0731- 205562
- Email: saev@saev.biz

La compilazione del seguente modulo non è vincolante ai fini di legge

Rag. Soc.			
Referente			
Città		Prov.	
Indirizzo			
Telefono		Fax	
E-mail			

Interessato a

- ☐ Corso approfondito Privacy (D.Lgs. 196/03)
- ☐ Corso Lotta Antincendio e gestione delle emergenze
- ☐ Corso Pronto Soccorso
- ☐ Corso per RSPP interno (Responsabile del servizio di prevenzione e protezione)
- ☐ Corso di Formazione per Addetti Carrellisti Elevatori
- ☐ Corso RLS (Rappresentate dei Lavoratori per la Sicurezza)

Desideriamo informarLa che, in osservanza del D.lgs. n. 196 del 30 giugno 2003 in materia di protezione dei dati personali, il trattamento dei suoi dati sarà improntato ai principi di correttezza, liceità e trasparenza e di tutela della sua riservatezza e dei Suoi diritti. Ai sensi dell'articolo 13, pertanto, La informiamo che i dati da Lei forniti verranno trattati informaticamente al solo fine di un corretto e esaustivo rapporto commerciale. Il conferimento dei dati è facoltativo, e l'eventuale rifiuto di fornire tali dati potrebbe comportare la mancata o parziale esecuzione del contratto oltre che alla mancata prosecuzione del rapporto. I Vs. dati non verranno diffusi e/o comunicati ad altri, sempre nei limiti del nostro rapporto commerciale. In relazione ai Vostri dati personali, potrete sempre e comunque esercitare i Vostri diritti previsti dall'Art. 7 del D. Lgs n. 196/2003, rivolgendovi direttamente alla Saev srl, con sede a Jesi in Via XV Settembre 16/a, che è il titolare del trattamento.

FIRMA_____

UN VERO AMICO LE PRENDE AL POSTO TUO.

IO LAVORO **SICURO.**

SICUREZZA. DOVERE ASSOLUTO, DIRITTO INTOCCABILE.

La sicurezza è un diritto che ogni datore di lavoro ha l'obbligo di garantire ai suoi lavoratori. E tu lavoratore pretendi gli strumenti di protezione, usali sempre, e denuncia chi mette a repentaglio la tua vita. Perché gli incidenti li puoi evitare, a te e agli altri. Per saperne di più vai su **www.iolavorosicuro.it**

PUBBLICITÀ PROGRESSO
Fondazione per la Comunicazione Sociale

Ministero del Lavoro, della Salute e delle Politiche Sociali