SAEV informa

Azienda di Servizi per la Privacy e Sicurezza sul Lavoro

La prima piattaforma in cloud per gestire la vostra Privacy

Rischi nel mondo del lavoro: videoterminali, rumore e radiazioni

Privacy: l'ondata del nuovo Regolamente Europeo

Videosorveglianza nel mirino del garante

IV Edizione - Ottobre 2013 - www.saev.biz

SAEV informa SOMMARIO

PRIVACY

5 Obblighi privacy per l'invio telematico delle dichiarazioni

5 Ancora problemi per facebook sulla privacy

6 Tutto quello che è pubblico sul web, senza che noi lo sappiamo

6 E' possibile inviare spot su social, Skype e WhatsApp solo se "Autorizzati"

7 Perplessità sulle ultime scelte legislative da parte del Garante Privacy

8 La videosorveglianza sempre di più nel mirino del Garante

8 Attenzione alle sanzioni sugli impianti di videosorveglianza

14 Un piano di educazione digitale da parte dei Garanti privacy

15 Licenziata, per vendicarsi cancella i dati aziendali

15 Le indicazioni del Garante per difendersi dallo spam

17 Occhio alla privacy con tablet e smartphone

18 Il parere del Garante sul Cloud Computing e la tutela dei dati

19 Marketing selvaggio: 800 mila euro di sanzioni a 3 società

19 208 ispezioni e 2.000.000,00 di Euro di sanzioni nel primo semestre

20 Varato il piano ispettivo del secondo semestre

20 Privacy: l'ondata del nuovo Regolamento Europeo

21 Controllo sui Pc aziendali Si, ma nel rispetto di precise regole

21 SHORT NEWS PRIVACY

SAEV

LA SAEV NEL FUTURO 23

LA NOSTRA PIATTAFORMA 25

LA CERTIFICAZIONE TÜV 27

SICUREZZA SUL LAVORO

28 I rischi nel mondo del lavoro: videoterminali, rumore e radiazioni

29 L'auricolare Bluetooth riduce gli effetti a carico del nervo uditivo rispetto al cellulare?

30 Il datore di lavoro è responsabile anche verso quei soggetti presenti solo occasionalmente in cantiere

30 Strage Viareggio, a giudizio tutti i 33 imputati

30 Un rischio biologico emergente: le endotossine aerodisperse

D.LGS 231/01 e 231/07

Cosè il D.Lgs 231/01? 31

Norme antiriciclaggio sui conti correnti 32

Il riciclaggio non conosce la recessione 33

Antiriciclaggio e tracciabilità del denaro. Come pagare in contanti 33

Pagamenti e antiriciclaggio: le ultime attività parlamentari 34

Obblighi privacy per l'invio telematico delle dichiarazioni

Gli intermediari alle prese con l'invio dell'Unico 2013 devono fare i conti con gli obblighi legati alla riservatezza dei dati o rischiano di vedersi revocata l'abilitazione a Entratel. Il processo di trasmissione deve tenere conto delle rigide regole sulla privacy che trovano applicazione sia nella fase propedeutica che in quella successiva di conservazione dei documenti. Chi trasmette le dichiarazioni deve dimostrare di essere in regola con la struttura organizzativa, che presuppone:

- la designazione degli incaricati del trattamento;
- l'esistenza della documentazione che attesta l'adozione delle misure minime di sicurezza (ex DPsS);
- l'adozione di una procedura di controllo nel rispetto degli obblighi previsti dal D.lgs 196/2003.

Devono inoltre essere adottate, per i supporti tecnologici, misure di sicurezza come:

- il blocco delle postazioni di lavoro quando si abbanndona la postazione di lavoro;
- l'installazione di programmi di protezione per mitigare i rischi di manomissione dei dati l'aggiornamento periodioco del sistema operativo e del software di protezione ;
- l'adozione di protocolli di sicurezza per limitare le intercettazioni delle reti wireless.

Infine, vanno verificate ulteriori misure di sicurezza, come:

- la conservazione delle dichiarazioni e dei documenti separatamente da quanto acquisito per altre attività;
- conservazione della documentazione fiscale con le modalità e per il periodo previsti dalla legge.

Ancora problemi per facebook sulla privacy

Non si arrestano i problemi sul fronte della gestione dei dati personali per il colosso Facebook.

L'ente governativo per la protezione dei consumatori, la Federal Trade Commission (FTC) ha aperto un'inchiesta sui recenti cambiamenti in materia di privacy fatti dal colosso, per capire se i nuovi termini violano l'accordo che prevede che gli utenti diano il consenso esplicito prima che le loro informazioni siano usate per pubblicità verso altri iscritti.

Il gruppo sostiene di avere il diritto di usare le informazioni dei profili e le immagini dei suoi iscritti per fare campagne pubblicitarie senza dare alcun compenso agli interessati.

Gli utenti e le associazioni hanno espresso indignazione anche per un cambiamento apportato alle politiche sulla privacy per i minori di anni 18 che, fornendo il loro consenso alle nuove regole, dichiarano che anche i loro genitori sono concordi con quanto firmato.

Le nuove regole sarebbero dovute entrare in vigore lo scorso 5 settembre, ma il colosso ha deciso di ritardarle proprio a causa delle polemiche.

Tutto quello che è pubblico sul web, senza che noi lo sappiamo

Gestire la privacy su internet richiede consapevolezza e attenzione. Ecco un vademecum minimo da ricordare quando si frequentano gli spazi pubblici di internet, come social network e blog.

Testi: I post dei blog e i messagi di Twitter sono progettati per essere visibili a chiunque su internet. I tweet possono essere cercati per mesi con motori di ricerca specializzati come Topsy. Nei social network un utente che scrive un messaggio oppure commenta deve ricordare di esaminare la visibilità del testo appena condiviso attraverso il pannello di controllo della privacy.

Fotografie: E' ormai facile archiviare vasti album su internet, ad esempio nei social network: gli utenti spesso sono in grado di gestire l'accessibilità da parte di altri per ogni singolo scatto. Inoltre attraverso le impostazioni delle privacy possono scegliere il grado di visibilità che preferiscono.

Filmati: Si moltiplicano le applicazioni software per girare video da smartphone e tablet come Tout, Viddy E Vine; è molto frequente che le registrazioni siano pubbliche come opzione predefinita. Inoltre i filmati possono essere rilanciati attraverso le reti sociali online e raggiungere una platea più ampia.

Profili Online: Ogni persona che si registra in un social network apre una pagina personale. Quasi sempre nelle grandi reti sociali virtuali gli iscritti possono scegliere tra una gamma di opzioni per la visibilità dei loro profili. E' sufficiente utilizzare un motore di ricerca per controllare se la propria pagina personale risulta visibile su Internet.

Gusti: Nelle reti sociali sul web è facile condividere con altri i propri interessi per musica, film, libri, videogame. Attraverso gli strumenti di controllo della privacy gli utenti possono valutare se vogliono che le loro preferenze siano visibili soltanto a se stessi, a gruppi predefiniti o a chiunque.

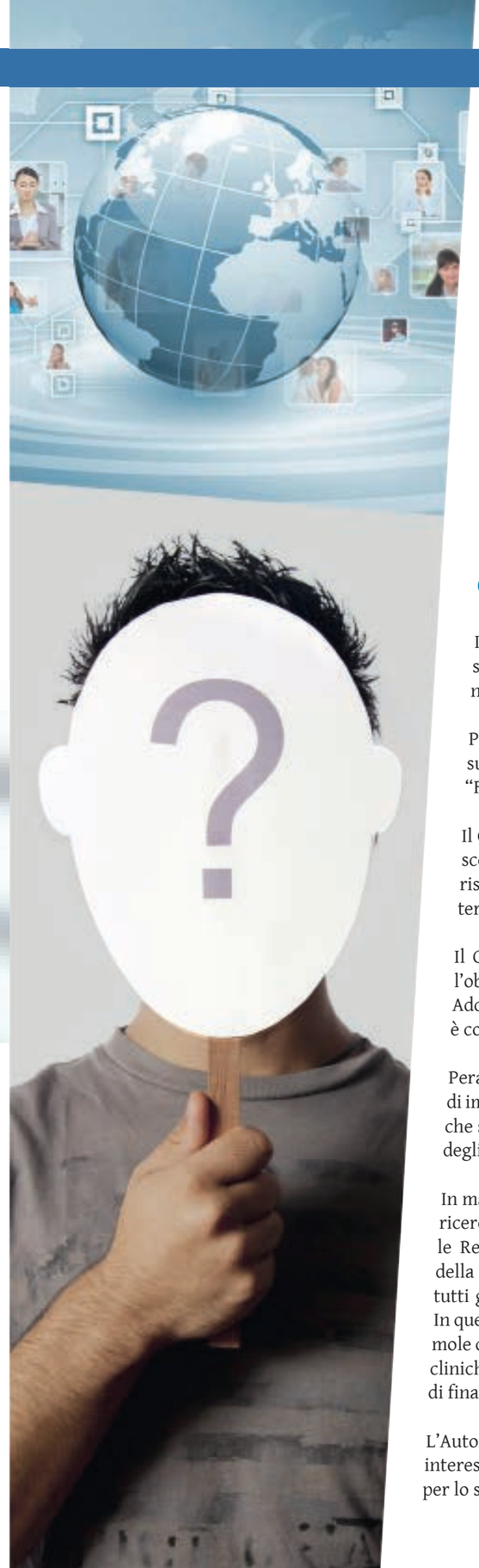
E' possibile inviare spot su social, Skype e WhatsApp solo se "Autorizzati"

E' possibile inviare la pubblicità sui social network solo a chi ha preventivamente epresso il consenso per riceverla. Lo ha deciso il Garante per la privacy, approvando le nuove linee guida in materia di attività promozionale e contrasto allo spam. L'obiettivo è combattere il marketing selvaggio e favorire pratiche commerciali che rispettino utenti e consumatori.

Il Garante, a tal proposito, vieta emails e sms indesiderati e impone maggiori controlli da parte di chi commissiona le campagne promozionali.

Il provvedimento definisce un quadro di misure e accorgimenti sia alle imprese che vogliono avviare campagne per pubblicizzare prodotti e servizi, sia a quanti desiderano difendersi dall'invadenza di chi utilizza senza il loro consenso recapiti e informazioni personali per tempestarli di pubblicità.

Il Garante ha stabilito che per inviare comunicazioni promozionali e materiale pubblicitario tramite sistemi automatizzati (telefonate preregistrate, email, fax, sms, mms) sarà necessario aver prima acquisito il consenso dei destinatari.
Servirà il consenso del destinario anche per l'invio di messaggi promozionali agli utenti di Facebook, Twitter e altri social network o di altri servizi di messaggistica e Voip sempre più diffusi come Skype, WhatsApp, Viber, Messenger. Il fatto che i dati siano accessibili su internet non significa che possano essere liberamente usati per



inviare comunicazioni promozionali automatizzate o per attività di marketing mirato. Il Garante consente, invece, l'invio di messaggi promozionali tramite email ai clienti su beni o servizi analoghi a quelli già acquistati e le promozioni per "fan" di marchi o aziende (ad esempio se un utente di un social network "segue" un brand, quell'azienda è autorizzata a inviargli offerte commerciali).

Le persone che ricevono spam possono presentare segnalazioni, reclami o ricorsi al Garante e comunque esercitare tutti i diritti previsti dal Codice della Privacy, inclusa la richiesta di sanzioni contro chi invia messaggi indesiderati. Nei casi più gravi le sanzioni possono arrivare fino a circa 500 mila euro. Anche le società possono comunque comunicare eventuali violazioni rivolgendosi all'Autorità Giudiziaria per azioni civili o penali contro gli spammer.

Perplessità sulle ultime scelte legislative da parte del Garante Privacy

Il Garante per la protezione dei dati personali ha richiamato l'attenzione sui rischi per la privacy dei cittadini che potrebbero derivare da alcune norme contenute nel recentissimo "Decreto del Fare".

Per quanto riguarda il "Decreto del Fare" due sono gli articoli che hanno suscitato forti perplessità, quello sul cosidetto "wi-fi libero" e quello sul "Fascicolo Sanitario Elettronico".

Il Garante ricorda che l'articolo 10 del decreto del fare n.69 del 21 giugno scorso, prevede che quanti offrono accessi a Internet tramite wi-fi (es. bar, ristoranti, alberghi) non debbano più identificare i clienti che utilizzano il terminale.

Il Garante ricorda che l'intervento sul cosidetto "wi-fi libero" stabilisce l'obbligo di tracciare alcune informazioni relative all'accesso alla rete (Mac Address) che sono dati personali in quanto sono riconducibili all'utente che è collegato a Internet.

Peraltro, l'adempimento richiesto, non solo grava su una platea considerevole di imprese, ma reintroduce obblighi di monitoraggio e registrazione dei dati, che sono stati preventivamente soppressi anche in ragione delle difficoltà e degli oneri legati alla loro applicazione.

In materia di Fascicolo Sanitario Elettronico (Fse) si prevede che per i fini di ricerca epidemiologica e di programmazione e controllo della spesa sanitaria, le Regioni, le Provincie autonome, il Ministero del lavoro e il Ministero della Salute possono accedere alle informazioni sanitarie presenti nel Fse di tutti gli assistiti, compresi i documenti clinici prima espressamente esclusi. In questo modo tali amministrazioni si troverebbero ad utilizzare una enorme mole di dati sensibili (ricoveri, accessi ambulatoriali, referti, risultati di analisi cliniche, farmaci prescritti) che non sono indispensabili per il raggiungimento di finalità diverse da quella della cura.

L'Autorità ha chiesto che la norma venga modificata affinchè i soggetti pubblici interessati possano accedere alle sole informazioni effettivamente necessarie per lo svolgimento di tali finalità.

GRUPPO FILENI
Distribuzione alimentare

COAL SOC. COP. ARL.
Rete di supermercati e distribuzione alimentare

A.N.P.AS. NAZIONALE
Le pubbliche assidtenze sul territorio

FALEGNAMERIA RAPONI
Produzione arredamenti e soluzioni su misura

OIKOS
Centro di solidarietà Onlus

LUCESOLE TRASLOCHI
Traslochi e Noleggio Piattaforme Aeree

GRUPPO FITIST
Vigilanza, scorta valori, portierato, guardania

GOMMUS SOC. COP. P.A.
Produzione suole in gomma

SARO
Lenti Oftalmiche

FONDAZIONE TEATRO STABILE MARCHE
Azienda agricola

FABITA
Cappe apirante ed Elettrodomestici

G&F CUCINE
Vendita diretta cucine componibili

IL MOLO
Ristorante Bar riviera Portonovo

STAMPA NOVA
Azienda grafica

CARP-ZONE
Carpfishing e Pesca Sportiva

ESISTAMPI
Stampi per materie plastiche

CONERO LUCIDATURE
Lucidatura e lavorazione argento e metalli

EUROSTOCK SENIGALLIA
Arredamento e prodotti per la casa

FISIOREUM
Ambulatorio fisioterapico reumatologico

SYSTEM DI ROSATI
Prodotti Elettromeccanici

EDILCASA MARCHI
Materiali ed accessori per l'edilizia

CREMERIA ROSA
Ristoramte - Bar - Cremeria

IL BIROCCIO SOC. COOP. AGR.
Servizi e Prodotti Agroalimentari

ROSCIANI SIRENA ASSEMBLAGGI
Assemblaggio e Cablaggio Impianti Elettronici

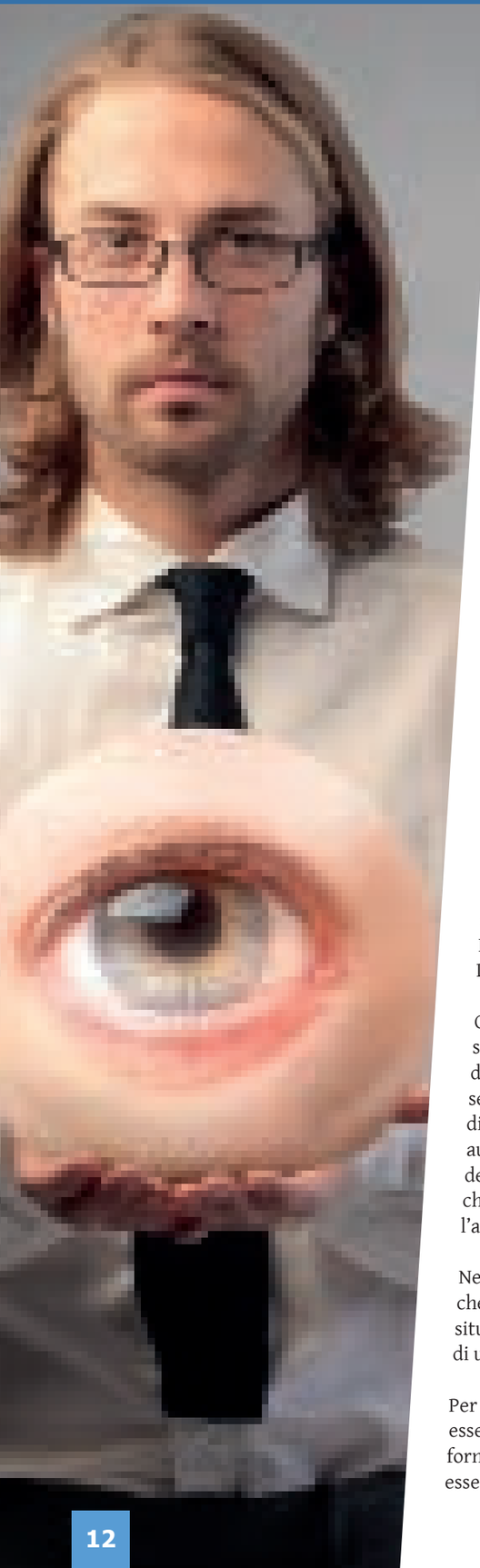
ROYALPREUS - GRUPPO GEMINI
Ruote in lega e Pneumatici

BODYLINE
Centro Fitness

N.E.T. IMPIANTI
Realizzazione Impianti Tecnologoci

DIESEL MARCHE
Riprazioni Veicoli Industriali

alcune REFERENZE SAEV



La videosorveglianza sempre di più nel mirino del Garante

L'autorità segnala che è cresciuto in maniera esponenziale l'utilizzo di tecnologie sofisticate e sistemi miniaturizzati, spesso camuffati che non rispettano quanto previsto dal Provvedimento Generale della Videosorveglianza. Le telecamere sono infatti posizionate nei luoghi più impensati, mascherate in ogni edificio pubblico. Scuole, stadi e ospedali sono setacciati centimetro per centimetro da occhi digitali.

Le esigenze di sicurezza sono cresciute, sulla base dell'emergenza criminalità, e ciò rende necessaria un'azione necessaria per verificare se ci siano delle violazioni.

Il Garante specifica che i controlli stanno avvenendo in collaborazione con il Comando di unità speciali della Guardia di Finanza; il fine delle verifiche è di controllare la conformità del funzionamento e dell'applicazione dei dispositivi di videosicurezza rispetto alle regole fissate dal Provvedimento Generale.

L'utilizzo dei sistemi di videosorveglianza nelle aziende sta attraversando una fase di sempre maggiore diffusione, sia in direzione di un efficace tutela del patrimonio aziendale, sia nell'ottica di un'accresciuta attenzione alla sicurezza dei lavoratori.

In questo senso la maggiore accessibilità (anche economica) di tecnologie sempre più efficienti ha sicuramente favorito la scelta di ricorrere alla videosorveglianza in alternativa o in aggiunta agli altri sistemi classici di tutela del patrimonio aziendale e/o controllo dell'attività produttiva.

Tuttavia gli aspetti giuridici coinvolti nella materia in oggetto, sono molteplici. In particolare devono essere analizzati due profili: il primo è quello connesso alla disciplina ex art 4 legge 300/70 (Statuto dei Lavoratori), il secondo è quello correlato alla tutela della riservatezza D.Lgs 196/2003.

Quanto al primo aspetto, infatti, la facoltà di installare le telecamere sul luogo di lavoro, è prevista, come eccezione ad un generale divieto di controllo a distanza dei lavoratori. Eccezione da intendere tuttavia in senso relativo, perchè in realtà la norma citata non prevede la possibilità di sorvegliare a distanza i lavoratori, ma ammette il ricorso ad impianti audiovisivi in presenza di esigenze organizzative, produttive e di sicurezza del lavoro nonché previo accordo con le rappresentanze sindacali aziendali che nel caso non siano presenti all'interno dell'azienda occorre chiedere l'autorizzazione alla Direzione Provinciale del Lavoro.

Nell'accordo dovranno essere specificati i motivi organizzativi e di sicurezza che impongono l'utilizzo di tali strumenti evidenziando la necessità di tale situazione, oltre all'indicazione del tipo di strumenti utilizzati e le modalità di utilizzazione.

Per quanto riguarda, l'aspetto relativo alla normativa sulla privacy devono essere rispettati il principio di proporzionalità e di correttezza, deve essere fornita un'adeguata informativa (anche sintetica) alle persone che possono essere riprese, deve essere determinato con precisione il periodo di eventuale conservazione delle immagini che non può comunque superare le 24 ore, e devono essere designati per iscritto i soggetti che possono utilizzare e prendere visione delle immagini.

Dunque, deve essere realizzato un sistema di videosorveglianza idoneo a controllare/riprendere solo quanto strettamente necessario e gestito in modo tale da garantire il controllo e prevenire l'abuso delle informazioni raccolte.

In crescita costante sono i ricorsi alle telecamere di controllo in aree aperte al pubblico e in aree private così come l'utilizzo di tecnologia sofisticate e sistemi miniaturizzati.

I problemi che spesso si riscontrano nell'ambiente che ci circonda, si affrontano in scala minore anche in quella piccola comunità che è il condominio.

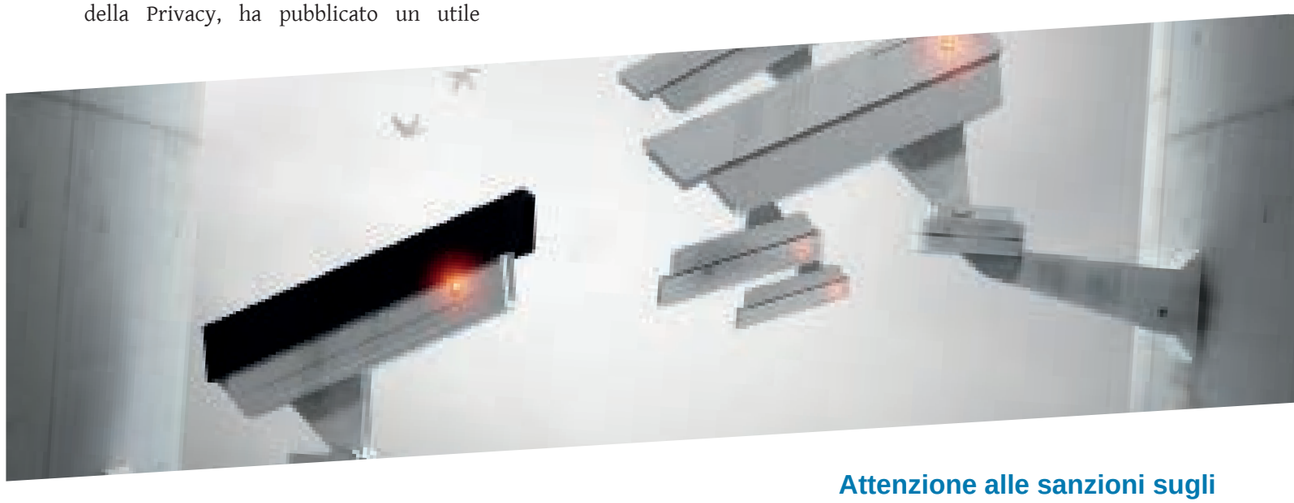
Così ci si può chiedere se un condomino ha il diritto o meno di installare una telecamere di videosorveglianza che riprenda il proprio posto auto o l'ingresso dell'appartamento.

Al fine di dissipare questo ed altri dubbi, il Garante della Privacy, ha pubblicato un utile Vademecum che si intitola "Il Condominio e la Privacy", che si prefigge di facilitare il dialogo tra i protagonisti di queste quotidiane vicende.

Con il manuale il Garante ha precisato che, per quanto riguarda la videosorveglianza in condominio, essa può interessare soltanto le aree comuni e deve seguire norme e limiti fissati dalla normativa generale sulla videosorveglianza.

Queste norme prevedono, ad esempio l'affissione di appositi cartelli, mentre le registrazioni dovrebbero essere conservate per un periodo non superiore a 24/48 ore a meno di specifiche esigenze legate alle attività presenti in condominio, come la chiusura di negozi ed uffici. In ogni caso, però, una conservazione superiore ai 7 giorni deve comunque sottostare al parere del Garante., tramite verifica preliminare per la quale non è valido il silenzio assenso.

La riforma ha introdotto una modifica per quel che riguarda il quorum necessario per deliberare l'installazione dell'impianto che prevede che ci sia la maggioranza degli intervenuti in assemblea e almeno la metà del valore millesimale dell'edificio.



Attenzione alle sanzioni sugli impianti di videosorveglianza

Molti impianti di videosorveglianza non rispettano quello che viene previsto dal Provvedimento sulla Videosorveglianza.

Spesso la multa è comminata per il mancato interesse del titolare o degli stessi installatori.

Ecco di seguito alcune sanzioni comminate:

Multa di 6.000,00 Euro ad un barista che aveva installato alcune telecamere all'interno e all'esterno del proprio locale con l'intenzione di garantire sicurezza al suo locale e prevenire azioni di malviventi, senza però segnalarne la presenza con un'informativa conforme allo schema indicato dal Garante.

Blocco delle videoriprese e in attesa della determinazione delle sanzioni, per un datore di lavoro che non ha sottoscritto un accordo con l'ispettorato in quanto le telecamere riprendevano i lavoratori durante la loro attività.

Sanzione di 1.600,00 Euro ad un datore di lavoro che, dopo aver già installato le telecamere voleva mettersi in regola, richiedendo l'autorizzazione all'Ispettorato del lavoro auto-denunciando un proprio comportamento illecito.

Il consiglio è quindi quello di rivolgersi ad installatori qualificati e a consulenti privacy specializzati, per avere le giuste indicazioni e non trovarsi successivamente a pagare una sanzione.

Un piano di educazione digitale da parte dei Garanti privacy

Le Autorità Garanti di tutto il mondo nella 35esima Conferenza internazionale sulla privacy hanno varato un piano di educazione digitale. La Conferenza ha adottato un programma, sostenuto con forza dal Garante italiano, che impegna a promuovere l'educazione digitale di tutti i cittadini, senza distinzione di età, esperienza o ruolo rivestito.

Il programma fissa cinque principi:

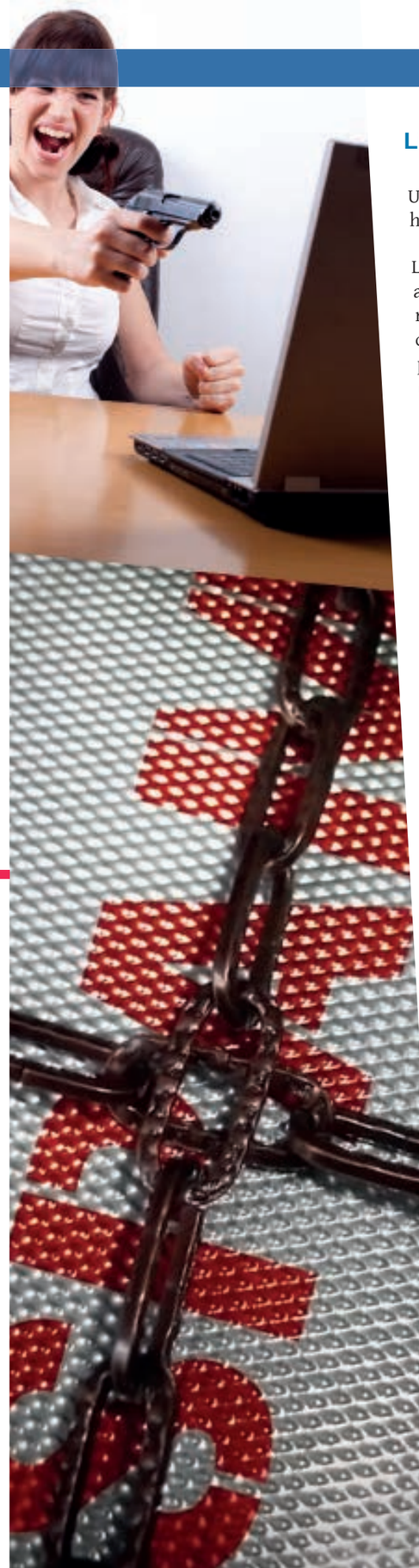
- Assicurare una protezione ai minori nel mondo digitale;
- Garantire una formazione sulla tecnologia digitale;
- Raggiungere un equilibrio tra opportunità e rischi presenti nella tecnologia digitale;
- Promuovere il rispetto degli utenti;
- Diffondere un pensiero critico sull'uso delle nuove tecnologie;

A sostegno di questi principi, sono stati individuati anche quattro obiettivi operativi:

- Promuovere un'educazione sulla privacy;
- Effettuare la formazione dei formatori, in materia di protezione dei dati personali;
- Sviluppare settori innovativi nel campo della "privacy by design";
- Formulare raccomandazioni e buone pratiche sull'uso delle nuove tecnologie a favore di genitori, insegnanti, minori e aziende;

All'interno della Conferenza sono state analizzate una serie di importanti questioni come:

- La necessità che imprese e governi assicurino la massima trasparenza nel trattamento dei cittadini;
- L'esigenza che l'attività di profilazione si basi su una preliminare valutazione di impatto-privacy, garantendo trasparenza agli interessati e ponendo particolare attenzione alla tutela dei minori;
- L'attenzione ai rischi legati al tracciamento della navigazione sul web, che deve essere reso più trasparente ed ispirarsi ai principi detti di "privacy by design";
- L'obietto di un maggiore coordinamento tra le Autorità per aumentare l'efficacia delle attività di enforcement;
- La necessità di adottare un piano strategico di azione per il biennio 2014-2015 finalizzato alla creazione di una rete globale di regolatori;
- La necessità di un accordo internazionale vincolante che salvaguardi i diritti umani attraverso un equilibrio tra sicurezza, interessi economici e libertà di espressione.



Licenziata, per vendicarsi cancella i dati aziendali

Un' ex impiegata, a seguito del suo licenziamento, non ci ha pensato due volte ed ha cancellato tutti i dati delle posizioni assicurative dei clienti.

La Polizia Postale, attraverso le indagini, ha denunciato la donna per accesso abusivo al sistema informatico, ma la cancellazione delle posizioni Inail di 37 rispettivi clienti, non è un grattacapo da poco, e neanche una bella figura per il commercialista che nel licenziare la donna pare essersi dimenticato che questa possedesse "le chiavi" per accedere indisturbata al sistema. Stando a quanto riferisce la Polizia Postale, la cessazione assicurativa delle ditte, clienti dello studio commercialista, avrebbe comportato il pagamento di un'ammenda complessiva di € 13.000.

Se da una parte l'ex dipendente passerà qualche guaio, non sono niente se paragonati a quelli dell'ex datore di lavoro, infatti il D.Lgs 196/2003, al punto 8 dell'Allegato B prescrive che le "le credenziali siano disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali", e pertanto il commercialista, in qualità di titolare del trattamento rischia l'imputazione per l'art.169 il quale prevede che "Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'art.33 è punito con l'arresto sino a due anni, oltre alla sanzione Amministrativa art.162 che comporta importi da 10.000 a 120.000 Euro. Su una cosa non c'è dubbio, se la donna voleva vendicarsi lasciando il segno al suo ex datore di lavoro, ci è riuscita appieno.

Le indicazioni del Garante per difendersi dallo spam

Spamming o spam è l'invio, tramite operatore o con modalità automatizzate, di comunicazioni non richieste (via telefono, email, fax, sms o mms), senza che il destinatario abbia ricevuto un'informativa sul trattamento dei dati personali o abbia prestato il consenso a ricevere messaggi.

Negli ultimi tempi, lo spamming sta interessando anche il mondo dei social network e quello dei sistemi di messaggistica per smartphone e tablet.
Lo spammer utilizza riferimenti (e-mail, numeri telefonici) mediante speciali programmi o facendo invii massivi a caso ad indirizzi mail basati sull'uso di nomi comuni.Scopo dello spamming è veicolare messaggi pubblicitari fino ad arrivare a veri e propri tentativi di truffa, come il phishing.

In Italia l'invio di messaggi automatizzati a fini promozionali non desiderati è soggetto a sanzioni amministrative e penali.

Differenze tra spam e invii leciti

Se il contatto e-mail o telefonico è stato raccolto con il consenso del destinatario o secondo le modalità previste dalla legge (es. nell'ambito di un contratto per la fornitura di un qualche servizio), non si può parlare di spam. In ogni caso, se le comunicazioni pubblicitarie o altro tipo di richieste (es. invio di newsletter) risultano ad un certo punto indesiderate, è tuo diritto opporti al trattamento dei dati inviando una mail al mittente per chiedere la sospensione dell'invio o utilizzare le procedure on-line per cancellare il tuo indirizzo email dal database di chi ti invia la comunicazione.

Come prevenire lo spam?

- **Non diffondere i tuoi indirizzi mail** o il numero di telefono fisso o mobile;
- **Leggi sempre con attenzione le regole privacy e le condizioni d'uso del servizio**, verificando le modalità e le finalità del trattamento dei tuoi dati personali;
- **Utilizza più indirizzi email per le tue varie esigenze**, creandone uno ad uso esclusivamente "commerciale" da impiegare per fare acquisti on line, accedere a servizi o iscriverti a newsletter;
- **Proteggi la tua mail con sistemi di crittografia** se vuoi pubblicarla sul tuo blog o sito personale;
- **Non rendere visibile gli indirizzi dei tuoi contatti,** quando invii una email a molti destinatari usa la funzione "destinatario in copia conoscenza nascosta";
- **Usare dei filtri anti-spam** offerti da alcuni programnmi di posta elettronica che permettono di cancellare tutta la posta proveniente da un particolare indirizzo;
- **Mantieni in efficienza il pc**, scaricando periodicamente gli aggiornamenti del sistema operativo e installa un programma anti-virus che offra anche una protezione anti-spam;
- **Se si utilizzano social network**:
  1. Controa le impostazioni privacy del tuo account eventualmente limitando la visibilità del tuo profilo;
  2. Utilizza la funzione di "blocco" per i soggetti che inviano messaggi indesiderati;
  3. Non dare l'amicizia a soggetti sconosciuti;
  4. Evita di rendere pubblici sulla tua pagina il tuo indirizzo e-mail o il tuo numero di cellulare.

Cosa non devi fare

- Non rispondere allo spam: l'email inviata in risposta può consentire allo spammer di stabilire che il tuo indirizzo email è valido e attivo;
- Non cliccare su eventuali link per la cancellazione dell'invio o su collegamenti ipertestuali inseriti nel corpo del testo;
- Non inserire i tuoi dati personali senza aver prima fatto delle verifiche;
- Non aprire allegati e non eseguire file con estensioni di tipo ".exe".

Come agire contro lo spam?

Se sei una persona fisica puoi presentare segnalazioni, reclami o ricorsi al Garante per la protezione dei dati personali e rivolgerti al giudice ordinario per l'eventuale risarcimento del danno.

Se sei una persona giuridica puoi rivolgerti al giudice ordinario per il risarcimento del danno ma non puoi fare segnalazioni, reclami o ricorsi al Garante che può però intervenire d'ufficio.

Occhio alla privacy con tablet e smartphone

Secondo un articolo pubblicato su Washington Post, tablet e smartphone multimediali ora hanno "una potenza di elaborazione maggiore rispetto a quella che nel 1965 aveva il Comando per la Difesa Aerea del Nordamerica".Tutti i modelli più diffusi permettono di collegarsi a internet, inviare e ricevere e-mail, fax e messaggi di testo, guardare la TV, ascoltare musica, fare fotografie e filmati, accedere a social network o spostarsi col navigatore satellitare. Attraverso il vostro affezionato smartphone passano fiumi di megabyte ogni giorno che si concretizzano in grandi quantità di informazioni personali e dati sensibili. In caso di tablet o smartphone aziendali, tutti gli addetti che li utilizzano devono essere appositamente nominati incaricati del trattamento dei dati personali ai sensi dell'art.30 del D.Lgs 196/2003 e dovranno essere adottate tutte le misure minime di sicurezza previste dal Codice. Ecco le principali:

- L'incaricato che accede dall'esterno alle banche dati deve poterlo fare solo previo inserimento delle proprie credenziali. Per rispettare questo parametro non è sufficiente il comune PIN.
- Redazione di un regolamento aziendale contenente precise istruzioni per il diligente uso e custodia dei palmari aziendali oltre alla cautele da adottare.
- Le password utilizzate dai dispositivi mobili devono essere composte da almeno 8 caratteri, non contenere riferimenti personali dell'incaricato, ed essere cambiate almeno ogni 6 mesi, oppure ogni 3 mesi, se la banca dati alla quale si accede contiene informazioni sensibili.
- Anche i palmari, come i comuni pc, devono essere impostati per effettuare aggiornamenti periodici forniti dal produttore.
- Se il palmare accede a banche dati residenti esclusivamente su server aziendali, non è necessario prevedere il backup dei dati. Mentre è obbligatorio effettuare il backup se tutti o anche solo parte dei dati sono memorizzati nella memoria dello stesso palmare.

Anche se rimossa dalle misure minime di sicurezza rimane obbligatoria la formazione degli incaricati che utilizzano dispositivi mobili aziendali, rimane una misura idonea. Le misure idonee, a differenza di quelle minime, non sono elencate da nessuna parte, ma sono ugualmente richieste dalla legge per evitare il rischio di pesanti risarcimenti. Individuarle è compito dell'azienda, sulla quale pesa la responsabilità dell'onere della prova, ovvero di dimostrare che ha fatto tutto il possibile per 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 (art. 31 del D.Lgs 196/2003).

Il parere del Garante sul Cloud Computing e la tutela dei dati

Uno dei termini più usati è sicuramente “cloud” (nuvola, in italiano). Con tale termine si fa riferimento a quell’insieme di tecnologie che permettono di utilizzare risorse hardware e software distribuite in remoto.

Un esempio di applicazione che funziona in the cloud è, Google Documenti che permette a tutti coloro che possiedono un account Google di elaborare documenti senza installare alcunchè sul personal computer, fruendo di tutti gli strumenti tipici di un wordprocessor tradizionale dalla finestra del browser. Lo stesso Gmail può essere considerato un servizio “in the cloud” dal momento che offre non soltanto funzionalità per la composizione, l’invio e la ricezione della posta elettronica ma anche per la sua gestione, organizzazione ed indicizzazione.

Il concetto cloud si riferisce a qualcosa che già esisteva anche in precedenza ad esempio quando un fornitore mette a disposizione uno spazio per allestire un sito web.
Nel servizio cloud c’è un fornitore del servizio (il cloud provider) e ci sono dei dati che vengono conservati su un server (o su un insieme di essi) disponibili ed accessibili in remoto. Un servizio cloud viene cucito in base alle esigenze dell’utente che può usare un’applicazione remota, installata sul server del cloud provider, che consente di assolvere ai compiti più disparati oppure un insieme di risorse software.
Occorre però muoversi con la massima cautela. Quando si caricano dei file “sulla nuvola”, è sempre bene proteggerli non affidandosi ai propositi ed alle dichiarazioni d’intenti del cloud provider.

Il Garante Privacy ha pubblicato un “vademecum” contenente una serie di indicazioni valide per tutti gli utenti, per imprese ed amministrazioni pubbliche per un utilizzo più ragionato degli strumenti disponibili “sulla nuvola”. L’obiettivo è quello di far riflettere su alcuni importanti aspetti giuridici, economici e tecnologici in una velocissima espansione e di promuovere un utilizzo corretto delle nuove modalità di erogazione dei servizi informatici.

L’adozione di tali strumenti presenta criticità e rischi per la privacy di cui è bene tenere conto. Prima di esternalizzare la gestione di dati e documenti o adottare nuovi modelli organizzativi è necessario scegliere con cura la soluzione più sicura per le attività istituzionali o per il proprio business.

Le prime vere novità in materia di tutela dei dati dovrebbero arrivare solo nel 2014 quando sarà approvato un Regolamento Europeo il quale supererà l’attuale Codice della Privacy italiano.
Sintanto che il nuovo Regolamento non entrerà in vigore, il garante spiega che l’azienda o la pubblica amministrazione “titolare del trattamento” deve designare il fornitore del servizio cloud come “responsabile del trattamento”.

Questo significa che il cliente dovrà sempre prestare molta attenzione a come saranno utilizzati e conservati i dati personali caricati sulla “nuvola” ed in caso di violazioni commesse dal fornitore, anche il titolare sarà chiamato a rispondere dell’eventuale illecito. Secondo il Garante non saranno scusabili nemmeno le realtà più piccole in quanto il cliente di servizi cloud può sempre rivolgersi ad altri fornitori che offrono maggiori garanzie, in particolare per il rispetto della normativa sulla protezione dei dati.

Il Garante Privacy chiarisce che il Codice vieta di trasferire dati personali fuori dall’Unione europea, anche a titolo temporaneo, qualora l’ordinamento del Paese di destinazione o di transito dei dati non assicuri un adeguato livello di tutela. Per le sue valutazioni il titolare del trattamento deve tenere conto anche del luogo dove vengono conservati i dati e quali sono i trattamenti previsti all’estero. Spetterà comunque sempre al titolare del trattamento dati verificare che le informazioni siano sempre accessibili, riservate e che siano assicurati i diritti di coloro che le conferiscono. Prima di rivolgersi ad un cloud provider il Garante consiglia di esaminare attentamente le misure di sicurezza adottate dal fornitore del servizio, di stabilire chi è il reale fornitore del servizio che si sta acquisendo, di raccogliere informazioni sulla disponibilità del servizio e sui piani di emergenza, sull’eventualità che i dati possano essere perduti, sulle garanzie di riservatezza, sulla collocazione dei server, sulla possibilità di migrare altrove tutte le informazioni o parte di esse e sulle eventuali assicurazioni danni.

Marketing selvaggio: 800 mila euro di sanzioni a 3 società

Il Garante della Privacy ha emesso tre ordinanze di ingiunzione per obbligare due importanti società di servizi informatici, specializzate nel settore delle banche dati al pagamento di sanzioni, pari a 800.000 euro, per aver violato provvedimenti prescritti già adottati nei loro confronti.

Nel corso di un’apposita attività ispettiva svolta dal garante è emerso che le due imprese specializzate nella creazione di banche dati, avevano realizzato e venduto archivi elettronici con i dati di decine di milioni di persone, sfruttando le informazioni conteneute negli elenchi telefonici prima del 2005 e nelle liste elettorali. Tali dati erano stati raccolti e utilizzati illecitamente , senza aver informato gli interessati e senza che questi avessero fornito uno specifico consenso ad attività di marketing o alla cessione delle loro informazioni personali ad altre società.

Per quanto riguarda invece l’operatore telefonico, dagli accertamenti è emerso che nonostante fosse a conoscenza dell’origine irregolare dei dati, li aveva comunque acquistati e utilizzati per contattare utenti e promuovere i propri prodotti e servizi tramite call center. Per tale attività dovrà pagare 300.000,00 euro.

208 ispezioni e 2.000.000,00 di Euro di sanzioni nel primo semestre

Poca informazione a utenti e clienti su come vengono usati e per quali scopi i loro dati, troppe informazioni personali trattate senza il consenso degli interessati, sopratutto da parte di società che si occupano di marketing telefonico.

Il bilancio dell’attività ispettiva e sanzionatoria del Garante nei primi sei mesi dell’anno è di 208 ispezioni e di 2 milioni di euro le somme riscosse da parte di soggetti pubblici e privati. Gli accertamenti hanno riguardato in particolare: il telemarketing, l’uso dei sistemi di localizzazione satellitare (gps) nell’ambito del rapporto di lavoro, il credito al consumo e le “centrali rischi” e le banche dati del fisco. Significativo il numero di procedimenti avviati: 473 procedimenti a fronte dei 578 dell’intero 2012. Le sanzioni hanno riguardato la omessa o inidonea informativa, il trattamento illecito dei dati legato principalmente al telemarketing e all’uso dei dati personali senza il consenso, mancata adozione delle misure di sicurezza , violazione del diritto di opposizione, omessa notifica al Garante e inosservanza dei provvedimenti dell’Autorità.

39 segnalazioni all’Autorità giudiziaria per violazioni dello Statuto dei Lavoratori, mancata adozione delle misure minime di sicurezza, trattamento illecito dei dati, false dichiarazioni e notificazioni al Garante o per inosservanza dei provvedimenti dell’Authority.

Varato il piano ispettivo del secondo semestre

Il Garante della Privacy ha varato il piano ispettivo per il secondo semestre 2013. Il piano prevede la prosecuzione dei controlli nel settore delle grandi banche dati pubbliche e l'avvio di ispezioni in ambiti particolarmente significativi come: attività di recupero crediti, formazione del Fascicolo Sanitario Elettronico, gestioni delle reti pubbliche di wi fi.

Circa 200 gli accertamenti ispettivi programmati che verranno effettuati anche in collaborazione con il Nucleo Speciale Privacy della Guardia di Finanza.

Privacy: l'ondata del nuovo Regolamento Europeo

Il Nuovo Regolamento Europeo si preannuncia una vera e propria rivoluzione, che sarà valido in tutta l'Unione andando a cambiare radicalmente i presenti scenari. Il principale risultato del Regolamento sul lungo periodo dovrebbe essere quello di garantire una maggiore semplificazione nei rapporti intracomunitari.

In questo clima di attesa, la domanda che tutti si pongono è: Cosa cambierà, sul piano concreto, con il nuovo Regolamento?

Le definizioni fondamentali restano invariate, ma con l'aggiunta del dato genetico e del dato biometrico. Il Regolamento sarà applicabile anche a chi, non facente parte dell'UE, tratta dati personali di cittadini dell'UE.

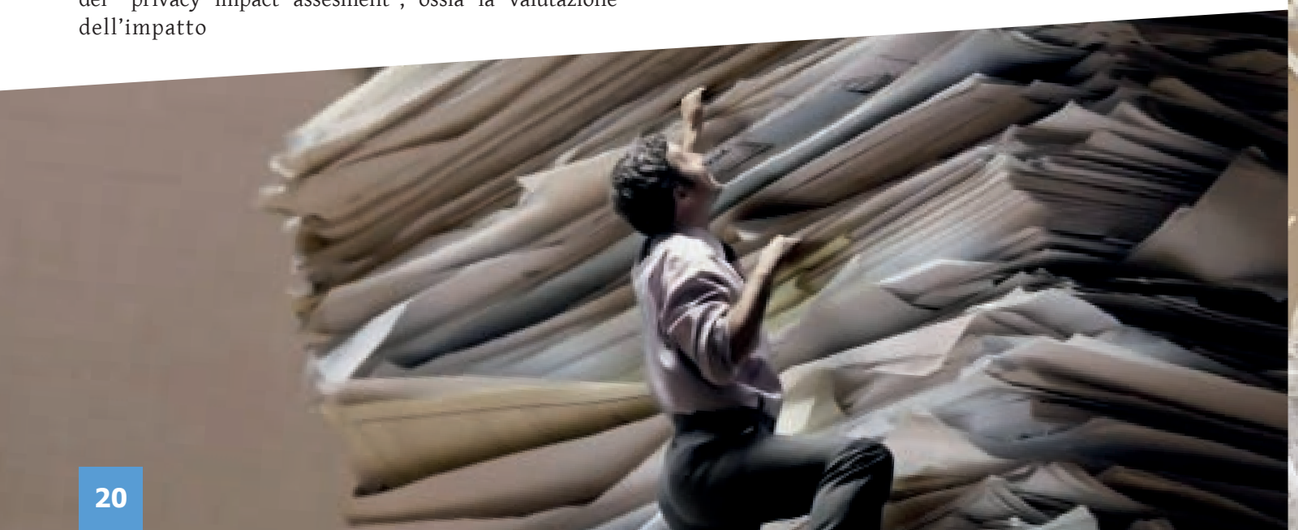
Non di secondaria importanza, l'introduzione del diritto degli interessati alla "portabilità del dato" da un provider all'altro e quello del "diritto all'oblio", vale a dire la facoltà per ogni interessato di decidere e richiedere la rimozione di informazioni e dati personali per motivi legittimi dopo un determinato periodo di tempo, per esigenze specifiche come la libertà di espressione o la possibilità di condurre ricerche storiche.

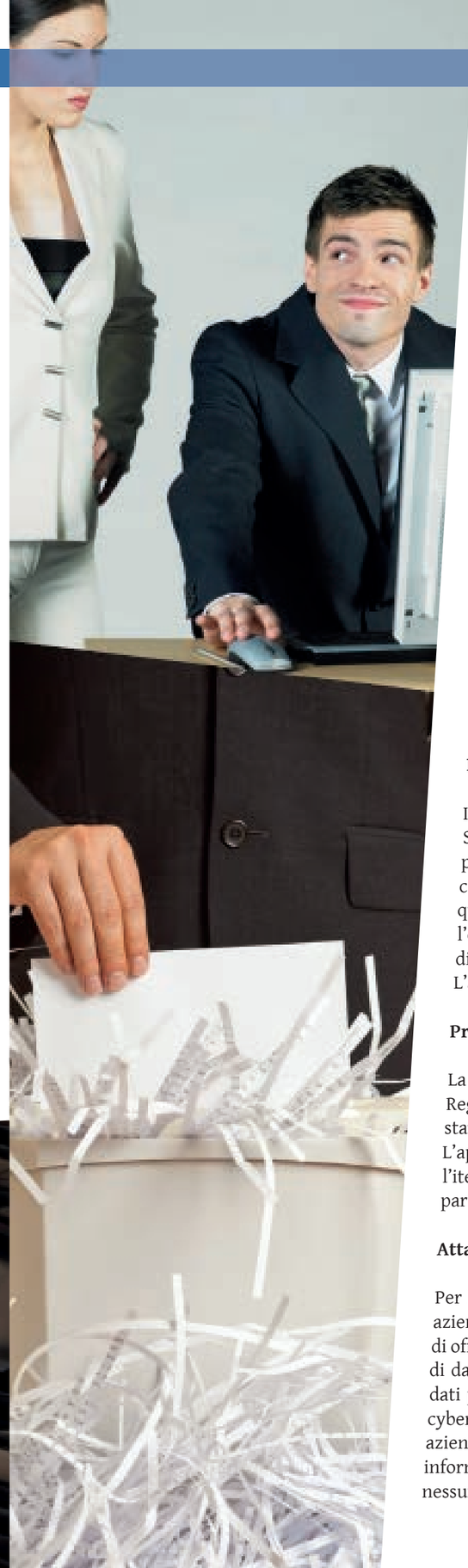
Oltre all'introduzione del "privacy by design", che impone la previsione di misure a protezione dei dati già al momento della progettazione del software o di un prodotto, e del "privacy impact assesment", ossia la valutazione dell'impatto privacy con riferimento all'avvio di un nuovo trattamento per alcune tipologie di dati (videosorveglianza, sanitari, biometrici, ecc.), tra le novità più rilevanti ricordiamo l'obbligo per talune aziende e per gli enti pubblici di nominare un "data protection officer", una nuova figura professionale a cui sono richieste competenze giuridiche ed informatiche in modo da poter organizzare nel modo più opportuno la gestione e tutela dei dati personali all'interno dell'azienda, nel rispetto della normativa.

Nel nuovo regolamento si parla anche della figura del "Joint Controller" o responsabile congiunto: nello specifico potranno sussitere due responsabili i quali saranno tenuti a concordare in un contratto il perimetro delle rispettive responsabilità privacy.

Le sanzioni previste sono altissime, fino ad un milione di Euro o il 2% del fatturato annuale di un'azienda a livello globale.

Non resta che attendere l'approvazione e verificare il testo finale. Appare però oppotuno, per le aziende e per il settore pubblico, cominciare a familiazzare con l'argomento, perchè non sarà certamente indolore passare da quattro adempimenti cartacei e qualche misura di sicurezza, ad una vera e propria organizzazione della sicurezza con reperimento di figure preparate sia sotto il profilo informatico, che organizzativo e normativo.





Controllo sui Pc aziendali Si, ma nel rispetto di precise regole

Una società non può controllare il contenuto del pc di un dipendente senza averlo informato di questa possibilità e senza il pieno rispetto della libertà e della dignità del lavoratore. Questa è la decisione del Garante sul ricorso presentato da un dipendente che era stato licenziato senza preavviso dalla propria azienda.

Dai riscontri è infatti emerso che la decisone del datore di lavoro era fondata su una serie di documenti contenuti in una cartella personale del pc portatile assegnato al lavoratore. La società vi aveva avuto accesso quando il dipendente aveva riportato il pc in azienda per la periodica operazione di salvataggio dei dati.

Il Garante ha ribadito che il datore di lavoro può effettuare controlli mirati sulla prestazione lavorativa ma sempre nel rispetto del lavoratore e della normativa privacy, informando il lavoratore tramite apposita informativa sul possibile trattamento dei suoi dati connesso all'attività di verifica e controllo.

SHORT NEWS PRIVACY

Redditometro all'esame privacy

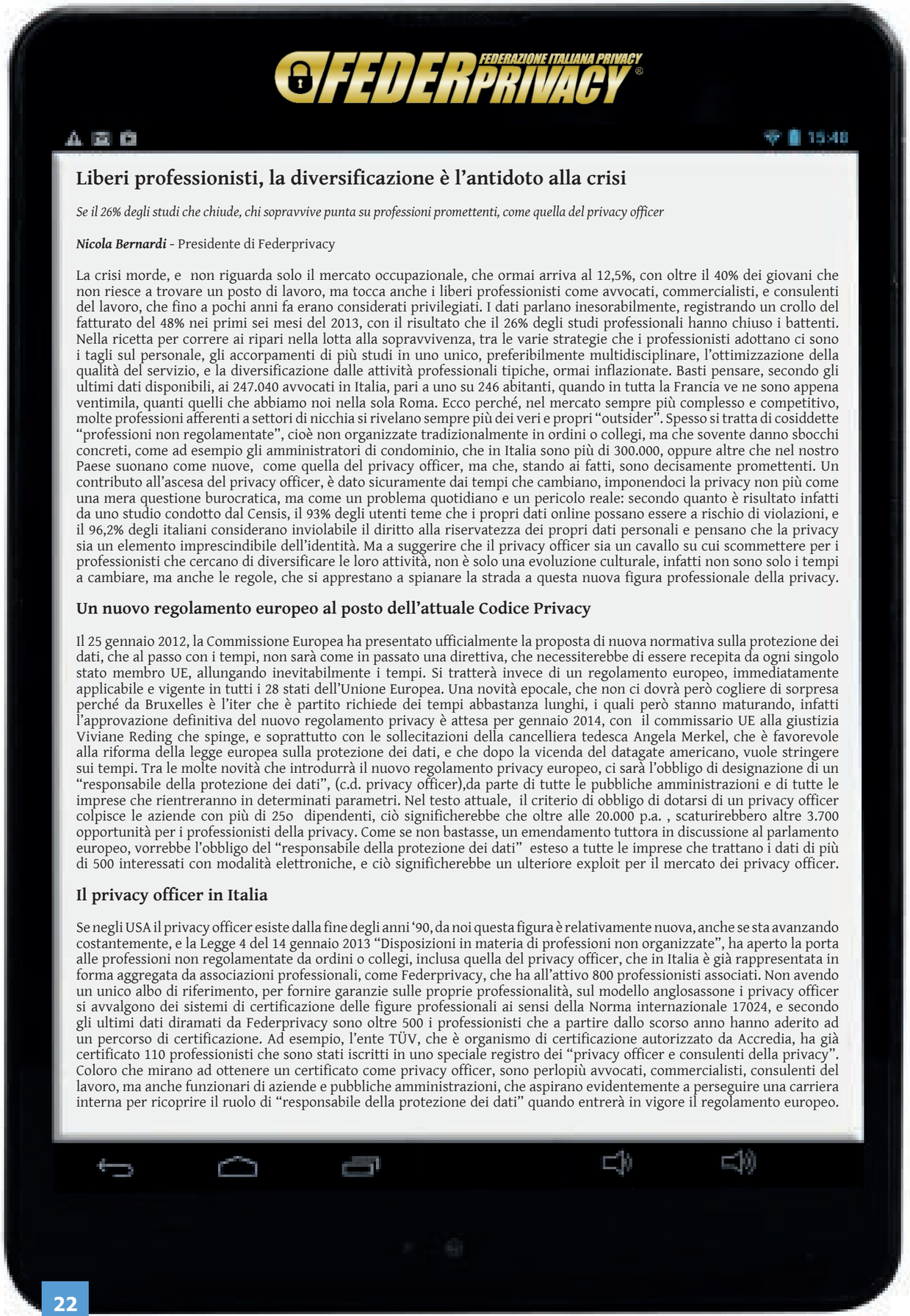
Il Garante della Privacy ha aperto un'istruttoria sul nuovo redditometro. Sotto osservazione ci sono sopratutto due aspetti. In primo luogo, la profilazione dei contribuenti, vale a dire le modalità con cui sono stati costruiti gli identikit e l'attribuzuione delle spese. In secondo luogo, la qualità dei dati presenti in Anagrafe tributaria, che consente di ricostruire l'effettiva capacità contributiva per metterla poi a confronto con i redditi dichiarati e valutare l'effettivo scostamento.
L'approfondimento dovrà portare all'emanazione di un provvedimento.

Priorità sull'emanazione del Regolamento Europeo

La Comnmissione Europea stà lavorando per introdurre il nuovo Regolamento Europeo sulla protezione dei dati che entrerà in vigore in 28 stati membri dell'Unione Europea.
L'approvazione del Regolamento Europeo, è adesso una priorità, in quanto l'iter deve essere portato a termine prima della fine del mandato dell'attuale parlamento, che andrà a scadere a giugno 2014.

Attacco ad Alpitur su Facebook

Per la prima volta in Italia è stato violato il profilo Facebook di una grande azienda, la Alpitur. Lo scopo era quello di diffondere, attraverso falsi annunci di offerte, programmi capaci di penetrare nel pc degli utenti per impossessarsi di dati importanti, come codici di carte di credito o credenziali di accesso e dati personali. L'attacco è iniziato la sera dell'11 settembre da un gruppo di cyber-criminali straniero, è durato oltre 48 ore ed stato denunciato dalla stessa azienda. La situazione adesso è stata risolta, ma per gli esperti di sicurezza informatica quanto è accaduto è un campanello di allarme perchè in Italia nessun gruppo criminale aveva preso di mira i social network.



LA SAEV NEL FUTURO

La SAEV è una società di servizi alle imprese, che opera principalmente nella provincia di Ancona, Pesaro e Macerata oltre ad alcune realtà a livello nazionale con oltre 600 clienti ad oggi attivi e circa 110 studi tra Commercialisti e Consulenti del Lavoro.

Oltre al servizio di consulenza, la SAEV organizza anche dei seminari di aggiornamento professionale, nei quali propone e approfondisce temi sempre attuali, e non solo in materia di privacy e sicurezza sul lavoro.

In uno degli ultimi incontri il principale relatore, il Dott. Chiaravalloti al momento Vice Garante della Privacy che ha accettato il nostro invito, ha sottolineato e plaudito, tra le altre cose, il nostro operato utile anche alla diffusione e sensibilizzazione della normativa privacy nel territorio, troppe volte trascurata e male interpretata.

Nel seminario organizzato nell'Ottobre 2013 oltre ad esaminare lo stato di adeguamento attuale alla normativa sulla privacy trattato dal Generale della Guardia di Finanza Gennaro Vecchione, si è approfondito un tema che in questo momento di crisi è estremamente attuale: il contenzioso tributario, che si è sviluppato in un interessante contradditorio tra il Prof. Tasini Massimiliano e il Dott.Viti Marco, funzionario dell'Agenzia delle Entrate di Ancona.

La SAEV è inoltre impegnata nel sociale con iniziative di solidarietà che scaturiscono oltre che da una propria sensibilità, anche dalla collaborazione con enti no profit quali ad esempio:

- Università dell'Aquila – 10 borse di studio per gli studenti vittime del terremoto
- Rotary Club di Jesi – Contributo di Solidarietà congiunto ai Terremotati dell'Emilia
- OIKOS di Jesi – Contributo di Solidarietà
- ANPAS Firenze – Adozione di n. 6 bambini della Tanzania
- Medici senza Frontiere – Donazione di n. 3 defibrillatori ed altri interventi minori

Dispone nel suo organico di Consulenti Privacy Certificati dalla TUV, che seguono il cliente con uno scrupoloso programma di interventi mirati, suddivisi in:

- **CONSULENZA PRIVACY:** Fase in cui viene fatta un'analisi approfondita della realtà aziendale per risolvere tutti gli obblighi in materia di privacy, ed

Futura sede operativa SAEV srl - Via Ignazio Filone, 1 - Jesi (AN)

in particolare nella stesura delle lettere di incarico, informative personalizzate, Disciplinare per posta elettronica e internet, Documenti Interni per l'Amministratore di Sistema e redazione del manuale Organizzativo Privacy;

- **ASSISTENZA ANNUALE**. Modellata secondo le esigenze dell'azienda in cui verranno effettuati tutti gli aggiornamenti tecnici e legislativi;

- **ASSUNZIONE DIRETTA DELLA RESPONSABILITA' AMMINISTRATIVA E CIVILE**, in caso di verifica da parte degli organi ispettivi, autorizzati al controllo;

- **CONSULENZA PER L'ADEGUAMENTO ALLA SICUREZZA SUL LAVORO** (D.Lgs. 81/08).

Il nostro obiettivo è quello di porci come consulente globale per l'adeguamento alla normativa privacy e alla sicurezza sul lavoro.

Tali normative occupano infatti un ruolo di primo piano nel panorama legislativo italiano/europeo e comporta significativi obblighi per imprese, enti pubblici e professionisti che spesso hanno forti difficoltà nell'identificare gli obblighi a cui sono soggette e le modalità con cui adeguarsi.
La nostra consulenza si basa sulla:

- Professionalità dei consulenti;
- Completezza del servizio;
- Sicurezza degli adempimenti.

La SAEV personalizza l'adeguamento sulla base della struttura e delle modalità operative del cliente. La consulenza tende in generale a sollevare il cliente da tutti gli adempimenti che possono essere gestiti in esterno, riducendo al minimo l'impatto della normativa sull'organizzazione aziendale interna in termini di tempo e di risorse umane/finanziarie impiegate. Il tutto garantendo:

- Il pieno rispetto della normativa;
- Un adeguato livello di protezione e riservatezza dei dati personali di clienti, fornitori, dipendenti, collaboratori;
- La valorizzazione del patrimonio dei dati aziendali in un'ottica di qualità del lavoro.

A garanzia dell'alto grado di professionalità la Saev si assume nei confronti del cliente, sia la responsabilità civile che amministrativa con un'adeguata polizza, stipulata grazie alla certificazione TUV.

LA NOSTRA PIATTAFORMA

SAEV ha introdotto uno strumento ICT (Information and Communications Technology) che, grazie alla tecnologia cloud, mette a disposizione dei clienti una piattaforma on line che consente all'azienda-cliente tramite un'area riservata per la consulenza diretta, una postazione riservata e protetta, collocata on-line, in grado di:

- Visualizzare e stampare il Modello Organizzativo Privacy;

- Visualizzare e stampare le nomine effettuate;

- Consultare e verificare l'elenco dei dati trattati;

- Consultare e verificare le misure di sicurezza adottate a livello elettronico;

- Consultare e verificare le misure di sicurezza adottate a livello cartaceo;

- Dare riscontro alle richieste ai sensi dell'art.7;

- Registrare e attestare le cessazioni di trattamento ai sensi dell'art.11 lettera e);

- Visualizzare e stampare il Disciplinare per Posta Elettronica e Internet;

- Visualizzare e stampare il manuale per l'utilizzo dell'impianto di Videosorveglianza;

- Effettuare formazione in modalità a distanza (e-learning);

- Accedere allo scadenzario che segnala, anche tramite mail, gli adempimenti in scadenza;

- Visualizzare e stampare le informative art.13, debitamente personalizzate;

- Stampare le lettere di incarico, con istruzioni agli incaricati, corredate da Linee guida per la Prevenzione dei Virus e la scelta delle password.

La piattaforma consente tramite il supporto on line e dei consulenti certificati, l'aggiornamento continuo della documentazione, la comunicazione immediata delle informazioni più rilevanti tramite newsletter e la revisione annuale di tutte le misure poste in essere, con conseguente rinnovo della documentazione.

La piattaforma fornisce anche una consulenza diretta on-line al cliente mediante apposita area riservata.

In tal modo la consulenza solleva il cliente da adempimenti che possono essere gestiti in esterno, riducendo al minimo l'impatto sull'organizzazione aziendale in termini di tempo, risorse umane e costi conseguenti.

Il tutto assicurando un elevato livello di protezione e riservatezza dei dati personali di clienti, fornitori, dipendenti e collaboratori, oltre alla valorizzazione del patrimonio dei dati aziendali in un'ottica di qualità del lavoro e di gestione della conoscenza (knowledge management).

Grazie alla piattaforma la SAEV permette al cliente di adempiere con completezza, puntualità e regolarità tutti gli obblighi della Privacy, senza che essi vengano percepiti come "problema" ma come elemento di qualità aziendale, affidando a SAEV il monitoraggio e l'assolvimento degli obblighi previsti con la certezza di essere sempre a norma.

La SAEV in seguito alle ultime novità legislative in campo della 231/01 ha messo in atto una piattaforma per la redazione del Modello Organizzativo previsto dalla norma.

I rischi nel mondo del lavoro: videoterminali, rumore e radiazioni

Sono diversi i rischi particolarmente diffusi nei luoghi di lavoro, ad esempio i rischi correlati all'attività dei videoterminalisti, alla presenza del rumore o alla presenza di radiazioni (anche se meno diffuso). Quando si parla di videoterminali, non stiamo parlando di tutte quelle attrezzature, come le calcolatrici o i registratori di cassa, che hanno un piccolo schermo per la visualizzazione dei dati forniti dalla macchina; quando si parla di videoterminale stiamo parlando di:

- Un lavoratore che utilizza l'attrezzatura munita di videoterminale (schermo alfanumerico o grafico) in modo sistematico e abituale per 20 ore settimanali;
- L'insieme delle attrezzature munite di videoterminale, eventualmente con tastiera e/o con altro sistema di immissione dati (incluso il mouse), il software per l'interfaccia uomo-macchina, gli accessori opzionali, le apparecchiature connesse (unità dischi, telefono, modem, stampante) il supporto per i documenti, la sedia, il piano di lavoro, nonché l'ambiente di lavoro immediatamente circostante.

Il legislatore ha tracciato un profilo prescrittivo per l'ambiente nel quale dovrebbe svolgersi il lavoro con uso sistematico di videoterminali:

- **Schermo:** i caratteri devono essere ben definiti, di forma chiara e grandezza sufficiente; l'immagine deve essere stabile e senza sfarfallamento; il contrasto e la luminosità devono essere regolabili; lo schermo orientabile e inclinabile, senza riflessi e riverberi modesti;
- **Tastiera**: inclinabile e separata dallo schermo, con una buona leggibilità dei simboli sui tasti; lo spazio deve essere sufficiente per l'appoggio delle mani e delle braccia; la superficie non riflettente;
- **Piano di lavoro**: abbastanza grande da consentire una disposizione flessibile di schermo e tastiera, dei documenti e del materiale accessorio e una posizione comoda; i supporti per documenti devono essere stabili e regolabili per ridurre al minimo i movimenti di testa e degli occhi;
- **Sedili di lavoro**: stabile, ma tale da consentire al lavoratore una posizione comoda e una certa libertà di movimenti, l'altezza deve essere regolabile e lo schienale deve essere regolabile sia in altezza che in inclinazione; poggiapiedi a richiesta.

L'eccesso di rumore oltre agli effetti sull'udito e extrauditivi ha anche effetti sull'attività lavorativa: "difficoltà della comunicazione verbale, diminuzione della vigilanza e dell'attenzione, calo di efficienza dovuto all'azione stancante esercitata dal rumore, perdita del controllo sull'ambiente". Si ricorda che l'allarme scatta quando l'esposizione quotidiana del lavoratore è pari o superiore a 80 db. Per quanto riguarda le radiazioni, è possibile suddividerli in **radiazioni non ionizzanti** (raggi X, raggi gamma e una parte dei raggi ultravioletti) e **radiazioni ionizzanti naturali** (onde a radiofrequenza, microonde e infrarossi). In particolare, laddove è presente il rischio, la protezione contro i raggi laser "si ottiene tenendo il locale schermato e chiuso con divieto di ingresso agli estranei, illuminato intensamente, ben ventilato e con superfici non riflettenti.

SICUREZZA SUL LAVORO

L'auricolare Bluetooth riduce gli effetti a carico del nervo uditivo rispetto al cellulare?

I potenziali effetti sulla salute associati all'utilizzo del telefono cellulare costituiscono da diverso tempo un argomento estremamente discusso e controverso. Numerosi studi sono stati condotti allo scopo di comprendere se l'uso frequente del telefono cellulare potesse essere correlato all'insorgenza di varie patologie specifiche a carico del cervello, del nervo acustico e del sistema uditivo in genere. Recentemente, un gruppo di scienziati dell'Università di Verona ha dimostrato che l'esposizione diretta ai campi elettromagnetici emessi dal terminale induce il deterioramento dei potenziali d'azione cocleari diretti del nervo. L'evidenza ha portato gli stessi autori a svolgere una indagine successiva, per verificare se questo effetto si riducesse utilizzando un dispositivo Bluetooth collegato al terminale mobile. Tale studio ha come scopo principale quello di comparare gli effetti di queste due differenti modalità di esposizione al campo a radiofrequenza (diretta o attraverso un auricolare Bluetooth) sul nervo uditivo e verificare se effettivamente il Bluetooth contribuisca a ridurre il deterioramento agendo di fatto come protezione alle funzionalità del sistema uditivo in toto. Dal minitoraggio è stato osservato che, aumentando la distanza tra telefono cellulare e orecchio, gli effetti a carico del nervo cocleare diminuiscono notevolmente, fino a perdere completamente di significatività ad una distanza di circa 50 cm. Considerando questi risultati, è quindi possibile affermare che l'utilizzo di un dispositivo Bluetooth collegato al terminale mobile tenuto in tasca o su un tavolo, costituisce una valida alternativa in termini di sicurezza all'uso del solo telefono cellulare.

Il datore di lavoro è responsabile anche verso quei soggetti presenti solo occasionalmente in cantiere

Il datore di lavoro ha l'obbligo di mettere in atto mìsure adeguate per la salvaguardia dei lavoratori e dei terzi ed è quindi responsabile di eventuali infortuni accaduti nel cantiere. Lo ha affermato la Corte di cassazione con la sentenza 6383/2013. A detta della Cassazione, nel cantiere la circolazione deve avvenire in modo sicuro; l'imprenditore deve perciò adottare tutte le misure per tutelare, non solo la salute dei lavoratori, ma anche quella dei terzi, cioè di altri soggetti presenti occasionalmente sul luogo dove si svolgono i lavori e privi dei presidi antinfortunistici. Gli infortuni dovuti a investimenti, a collisioni macchine-pedoni, che avvengono nei luoghi di lavoro in prossimità di macchine mobili, sono ancora molto numerosi, specialmenete nel comparto edile con le macchine da cantiere, nel comparto della raccolta e cernita dei rifiuti e nella movimentazione con carrelli semoventi. Senza dimenticare che molti infortuni non stradali che accadono a conducenti di automezzi dipendono dalla caduta che si verifica nelle fasi di salita o discesa dai mezzi. La prevenzione delle collissioni macchine-pedoni può essere realizzata in primo luogo con misure organizzative e con il miglioramento della visibilità. Per integrare queste misure, nel caso dovessero rivelartsi insufficienti a garantire la sicurezza delle persone, si può ricorrere ad alcune misure tecniche complementari come l'installazione di rilevatori di persone. Ogni azienda deve definire il bisogno di questi sistemi di rilevazione prima della loro installazione, in particolare è necessario:

- identificare ogni situazione intorno al veicolo (movimenti della macchina che presentano dei rischi significativi per le persone, fasi particolari dei movimenti che peresentano dei rischi significativi per le persone, zona a rischio attorno alla macchina dove circolano o stazionano persone);
- stimare il livello di rischio di ogni situazione rischiosa (frequenza e durata dell'esposizione delle persone a rischio);
- studiare la possibilità di ricorrere a un dispositivo di segnalazione delle persone;
- specificare tecnicamente la o le caratteristiche della segnalazione (taglia dell'oggetto da intercettare, distanza di intercettazione, dimensione, localizzazione della/e zone da segnalare, tempi di risposta richiesti);
- scegliere e mettere in pratica una soluzione tecnica;
- valutare le misure installate (considerando il punto di vista delle diverse persone coinvolte per conoscere il loro grado di soddisfazione rispetto al dispositivo installato).

Strage Viareggio, a giudizio tutti i 33 imputati

Il gup di Lucca Alessandro dal Torrione ha rinviato a giudizio tutti i 33 imputati nel procedimento per la strage di Viareggio. La strage avvenne il 29 giugno 2009: un treno carico di gpl deragliò attraversando la stazione, alcune cisterne si ribaltarono e una si squarciò. Il gas fuoriuscito esplose devastando un quartiere e uccidendo 32 persone: 11 sul colpo altre 2 per infarto e le restanti per l'aggravarsi delle ustioni riportate nell'incidente.

Fra i reati ipotizzati dalla Procura, il disastro colposo, l'incendio colposo, l'omicidio e le lesioni colpose plurime. Ad alcune imputati sono state contestate anche violazioni delle norme sulla sicurezza sul lavoro. Il processo si aprirà il 13 novembre a Lucca.

Un rischio biologico emergente: le endotossine aerodisperse

Le endotossine vengono rilasciate in piccole quantità nell'ambiente durante la normale crescita batterica ma, nella maggioranza dei casi, vi rimangono associate fino alla morte del microorganismo e per tale ragione risultano essere frequenti le contaminazioni ambientali.

L'esposizione ad endotossine è comune in diversi settori occupazionali, ma risulta prevalente in alcuni ambienti lavorativi nei quali la manipolazione di materiale organico contribuisce allo sviluppo di polveri di cui le endotossine risultano essere una componenete biologicamente attiva:

- Industrie agricole e zootecniche;
- Industrie tessili;
- Impianti di macellazione;
- Impianti di trattamento di acque reflue, rifiuti solidi urbani e rifiuti vegetali;
- Falegnamerie.

Le endotossine giocano un ruolo importante nello sviluppo di patologie respiratorie correlate alla presenza di polveri organiche nell'ambiente lavorativo.

La loro inalazione può indurre reazioni infiammatorie e tossiche causando febbre, alterazioni cardio-vascolari e alterazioni delle funzioni polmonari con conseguenti complicanze respiratorie quali tosse, respiro affannoso e insufficenza toracica. Un'esposizione prolungata può determinare diminuzione cronica delle funzioni polmonari.

L'Agenzia Europea per la Sicurezza e la Salute sul Lavoro con il relativo osservatorio europeo hanno svolto un'indagine sul tema dei rischi emergenti al fine di permetterne la tempestiva individuazione e consentire il raggiungimento di una migliore pianificazione degli interventi di prevenzione.

L'esposizione ad endotossine rientra nei primi 10 rischi biologici emergenti. Questo per due ragioni:

- Ampliamento della popolazione a rischio: elevate concentrazioni di endotossine sono state riscontrate anche in ambienti indoor adibiti ad uso ufficio, scuole ed abitazioni private, a seguito della contaminazione dei sistemi di ventilazione ed umidificatori da parte di batteri gram-negativi;

- Recentemente sono stati segnalati effetti clinici più severi (bronchiti croniche, allergie, crisi asmatiche, sindrome da polvere organica tossica, shock settico e insufficenza di alcuni organi)

Attualmente non sono disponibili procedure standardizzate ed universalmente riconosciute in merito alla misurazione delle endotossine ambientali.
L'esposizione ad endotossine aerodisperse è un evento strettamente connesso con la tipolgia lavorativa.

Tuttavia, per ridurre significativamente il livello di esposizione, sopratutto in ambienti confinati (indoor), possono essere messe in atto delle misure di prevenzione e controllo:

- Misure igieniche generali (es. accurata igiene delle mani);

- Misure specifiche: manutenzione periodica degli impianti di trattamento aria, adeguato sistema di filtrazione, idoneo ricambio aria dei locali e di aspirazione dell'aria esausta, sistemi di aspirazione localizzati in punti critici;

- Misure organizzative: riduzione, ove possibile, dei tempi di permanenza in aree ad alto rischio di esposizione;

- Adozione di mezzi di protezione individuale delle vie respiratorie (es. facciali filtranti);

- Informazione e formazione del personale addetto.

Cosè il D.Lgs 231/01?

Il Decreto Legislativo 8 giugno 2001, n.231, recante "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, ha introdotto per la prima volta la responsabilità in sede penale degli enti, che si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto illecito, a "vantaggio dell'organizzazione" o "nell'interesse dell'organizzazione" senza che ne sia ancora derivato necessariamente un vantaggio concreto.
Quanto sopra citato vale sia che il reato sia commesso da soggetti in posizione apicale che da soggetti sottoposti all'altrui direzione, inclusi i soggetti come consulenti o procacciatori.
La società non risponde se le persone indicate hanno agito nell'interesse esclusivo proprio o di terzi.
L'ampliamento della responsabilità mira a coinvolgere il patrimonio degli enti e gli interessi economici dei soci, i quali non pativano conseguenze dalla realizzazione di reati commessi.
L'innovazione normativa non è di poco conto in quanto né l'ente, né i soci delle società possono dirsi estranei al procedimento penale per reati commessi a vantaggio o nell'interesse dell'ente.
Le fattispecie di reato rilevanti possono essere comprese nelle seguenti categorie:
1. Delitti contro la pubblica amministrazione (corruzione, truffa ai danni dello Stato, frode informatica ai danni dello Stato) o contro la fede pubblica (falsità in monete, carte di pubblico credito, valori di bollo e in strumenti o segni di riconoscimento);
2. Reati societari (false comunicazioni sociali, falso in prospetto, illecita influenza sull'assemblea);
3. Delitti in materia di terrorismo e di eversione dell'ordine democratico (ivi incluso il finanziamento ai suddetti fini);
4. Delitti contro la personalità individuale (sfruttamento della prostituzione, pornografia minorile, tratta di persone, riduzione e mantenimento in schiavitù);
5. Abusi di mercato;
6. Pratiche di mutilazione degli organi genitali femminili;
7. Reati Trasnazionali (associazione a delinquere, associazione finalizzata al contrabbando di tabacchi lavorati esteri, traffico illecito di sostanze stupefacenti o psicotrope, riciclaggio, impiego di denaro beni o altrà utilità di provenienza illecita, traffico di migranti ed alcuni reati di intralcio alla giustizia che rivestono carattere di transnazionalità);
8. Omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro;
9. Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita;
10. Delitti informatici ed illecito trattamento dei dati;
11. Delitti di criminalità organizzata;
12. Delitti contro l'industria e il commercio;
13. Delitti in materia di violazioni del diritto d'autore;
14. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;

15. Reati ambientali ed inquinamento del mare da parte delle navi;
16. Impiego di lavoratori stranieri irregolari;
17. Corruzione tra privati;

Le sanzioni previste dal D.Lgs 196/2003 sono:
1. Pecuniarie;
2. Interdittive;
3. La confisca;
4. Pubblicazione della sentenza;

Le sanzioni pecuniarie si aggirano da un minimo di 25.800,00 € ad un massimo di 1.549.000 €, salvo riduzioni.

Le sanzioni interdittive sono:
1. L'interdizione dall'esercizio dell'attività;
2. la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
3. il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni d'un pubblico servizio;
4. l'esclusione da agevolazioni, finanziamenti, contribuiti o sussidi e l'eventuale revoca di quelli già concessioni;
5. divieto di pubblicizzare beni o servizi;

Il legislatore ha previsto la possibilità per l'ente di sottrarsi totalmente o parzialmente all'applicazione delle sanzioni se dimostra, in occasione di un procedimento penale per uno dei retai considerati, di aver adottato ed efficacemente attuato Modelli di organizzazione, gestione e controllo idonei a prevenire la realizzazione degli illeciti penali considerati.
La mancata adozione del Modello non è soggetta ad alcuna sanzione, ma espone l'ente alla responsabilità per gli illeciti realizzati nel suo interesse.L'adozione diviene pertanto obbligatoria se si vuole beneficiare dell'esimente escludendo la colpa organizzativa. Alcuni Enti Pubblici, non stipuleranno più convenzioni con organizzazioni non dotate di Modelli Organizzativi 231.

Norme antiriciclaggio sui conti correnti

Molti correntisti italiani potrebbero ricevere una lettera dal proprio istituto di credito, contenente l'invito a trasmettere una serie di dati sulla propria identità. Sarà meglio non cestinare la lettera, in quanto il conto corrente potrebbe essere bloccato se la banca non riuscisse a condurre l'operazione di verifica sul cliente. In base alle nuove norme antiriciclaggio la banca deve obbligatoriamente restituire denaro, titoli e altri strumenti finanziari se non riesce a completare la verifica sul cliente. Finora questo procedimento era stato sospeso, a causa dell'assenza delle procedure attuative.

Ora che sono state emanate dalla circolare del 30 luglio 2013, per opera del ministero dell'economia, le banche dovranno effettuare la verifica dei dati del cliente per adempiere agli obblighi antiriciclaggio. Se il cliente non consente il completamento della verifica entro un termine ragionevole o addirittura si rifiuta di collaborare, la banca può bloccare il conto corrente.

Il correntista non potrà effettuare nessun tipo di operazione bancaria, avverrà la restituzione delle disponibilità finanziarie, la revoca automatica degli assegni e addirittura la chiusura del rapporto con l'istituto di credito.
Se il correntista non avrà in ogni caso consentito alla banca di accertare i dati, allora l'istituto di credito dovrà inviare al cliente una comunicazione scritta nella quale far presente l'obbligo di astensione e la necessità di ottenre, entro 60 giorni dalla ricezione della comunicazione, le coordinate bancarie per poter restituire le disponibilità del cliente. Il conto corrente indicato dal cliente per la restituzione del denaro dovrà essere a lui intestato o tuttalpiù cointestato.

Il riciclaggio non conosce la recessione

Il riciclaggio non conosce crisi. Un miliardo di euro fatto transitare su conti di società in paradisi fiscali per poi approdare a San Marino. Un'operazione su cui la Procura di Roma e il nucleo polizia valutaria della Guardia di Finanza hanno acceso i fari confermando ancora una volta il contrasto al traffico di denaro "sporco" e l'evasione fiscale internazionale siano strettamente connessi. Un'indagine che va ad incrementare il già ricco tesoro portato alla luce dall'inizio dell'anno. Il conteggio ufficiale parla di quasi quattro miliardi di euro tra denaro, titoli e altri valori pregiati trasferiti illegalmente scoperti da gennaio a fine maggio. Tra i settori più controllati e sotto oservazione ci sono i money transfer e i compro oro, che spesso mettono in atto condotte non in linea con le regole antiriciclaggio. C'è poi l'evergreen delle violazioni riscontrate alla frontiera, per le quali il nemico numero uno è rappresentato dalle banconote di grosso taglio. Le nuove regole introdotte hanno portato a un aumento di oltre un terzo delle violazioni riscontrate.

I controlli mirati partono dall'incrocio dei dati spesso raccolti proprio presso le dogane per poi sviluppare indagini mirate e approfondite, viene tracciato l'identikit dei soggetti per poi incrociarlo con la posizione reddituale e procedere a ulteriori riscontri. Altro segnale in stretta connessione con la crisi è rappresentato dall'intermediazione finanziaria abusiva. Un'attività in forte crescita, in cui operano soggetti privi di qualsiasi requisito di onorabilità e che nei casi maggiori porta a scoprire grandi reati legati all'usura. L'alto livello di attenzione sul riciclaggio da parte della Guardia di Finanza deriva anche dalle segnalazioni di operazioni sospette arrivate dall'Unita di Informazione Finanziaria presso la Banca d'Italia. Nel 2012 sono stati quasi 60 mila gli imput di sospetto di traffico di denaro illecito trasmessi al nucleo di polizia valutaria delle Fiamme Gialle, mentre nei primi mesi di quest'anno ne sono state approfondite quasi 5.500. Un aspetto sotto la lente di ingrandimento sono le segnalazioni dei professionisti. Già da qualche anno la Guardia di finanza pianifica una serie di controlli per verificare il rispetto degli obblighi antiriciclaggio da parte degli studi. Aspetti su cui, anche i Consigli nazionali degli Ordini si stanno sempre più muovendo con check-list e istruzioni agli iscritti su controlli e adempimenti da rispettare.

Antiriciclaggio e tracciabilità del denaro. Come pagare in contanti

Riguardo le norme antiriciclaggio, è bene notare che è possibile effettuare pagamenti in più rate attraverso denaro contante, senza violare le leggi, ed è anche lecito pagare una rata per contanti e la residua parte attraverso sistemi che garantiscono la tracciabilità. L'aggiramento del limite di euro 999,99 al trasferimento di contante fra soggetti diversi, operato attraverso il frazionamento della somma inerente la stessa operazione economica in tante parti in modo che ciascuna sia di importo inferiore alla soglia indicata, non è consentito dalla legge. L'attività in questione sarebbe considerata elusiva delle norme stabilite. Tuttavia se l'operazione di frazionamento è prevista dalla natura dell'operazione ovvero deriva da un preventivo accordo tra le parti e per ogni singolo pagamento viene conservata disposizione scritta dei contraenti, la condotta in oggetto non configura azione illecita. Si ricorda che, ad eccezione delle soglie stabilite da ciascun istituto e della disponibilità personale sul deposito, non esistono limiti al versamento e al prelevamento di denaro dal proprio conto corrente, poiché interviene l'intermediario bancario e non si realizza trasferimento da un soggetto all'altro. Tuttavia il personale bancario, è obbligato a registrare le operazioni sopra la soglia consentita e a valutare la presenza di fattori di anomalia per decidere eventualmente di far scattare la segnalazione di operazione sospetta, destinata all'Unità di Informazione Finanziaria.

Pagamenti e antiriciclaggio: le ultime attività parlamentari

La Banca d'Italia ha emanato le disposizioni attuative in materia di adeguata verifica della clientela che le banche e gli intermediari finanziari devono adottare a fini di prevenzione e contrasto del riciclaggio e del finanziamento al terrorismo, in applicazione della normativa antiriciclaggio (D.Lgs 231/2007).

Il provvedimento prevede:

- una verifica rafforzata per le persone politicamente esposte;
- controlli sui conti delle società operanti nei settori degli appalti, della sanità, dei rifiuti e delle energie rinnovabili;
- l'identificazione dei titolari effettivi dei rapporti con gli intermediari;
- verifica delle operazioni di deposito, prelievo e pagamento che hanno come oggetto le banconote da 200 a 500 euro.

Il provvedimento entrerà in vigore il 1° gennaio 2014. Le uniche attività escluse sono le imprese di assicurazione.

Sono stati disciplinati due casi in cui è possibile derogare al generale divieto di utilizzo contante dai 1.000 €:

- Il **D.L 16/2012** ha previsto che gli **operatori del settore del commercio al minuto e agenzie di viaggio e turismo** possono vendere beni e servizi a cittadini stranieri non residenti in Italia, entro il limite di 15.000 €, in deroga alle norme sulla limitazione all'uso del contante, utilizzando un'apposita **procedura**;
- Il **D.Lgs 169/2012** ha elevato a 2.500 € la soglia per le **attività svolte dai cambiavalute con i clienti**.

Tutto
molto funzionale

Tuttolavoro Suite è la soluzione informativa on line che ti permette di consultare in modo semplice e immediato, da un unico punto di accesso, tutti i contenuti in materia di lavoro indispensabili per la tua attività professionale.

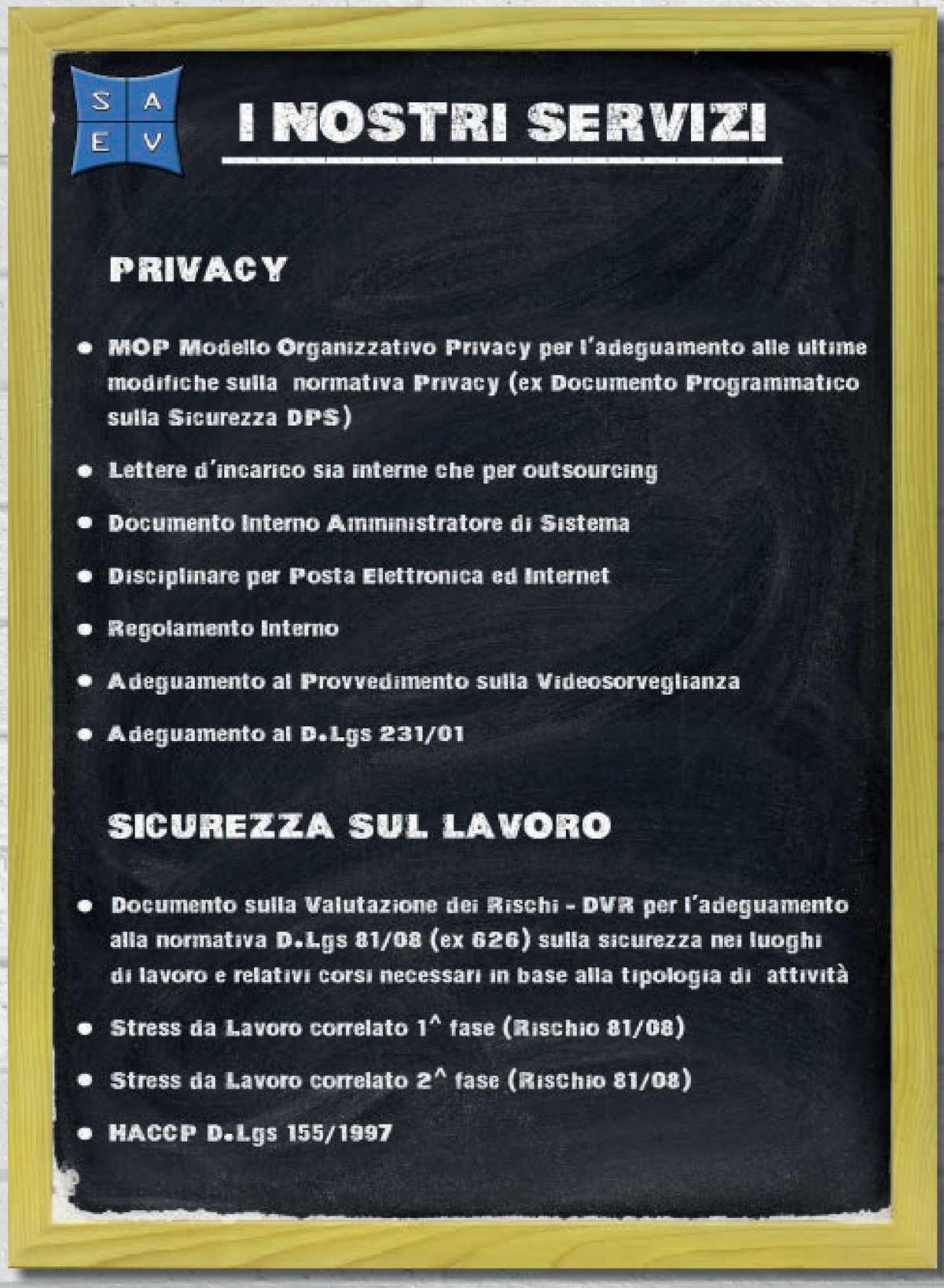
Tutto Lavoro
INDICITALIA Suite

Con TuttoLavoro Suite puoi configurare la soluzione più adatta alle tue esigenze, a partire dalla banca dati sino ai singoli moduli complementari, che approfondiscono argomenti di specifico interesse: notizie quotidiane, approfondimenti e commenti d'autore, casi risolti dell'Esperto, disciplina sanzionatoria, previdenziale e sulla privacy, formule e modelli, procedure di calcolo e per l'elaborazione del costo del lavoro.

Da oggi scegli quello che vuoi

Wolters Kluwer Italia

www.indicitalia.it/tuttolavoro



Consulenti Privacy e Privacy Officer Certificati

TÜV SÜD

Consulenza e servizi per l'adeguamento alle normative in materia di privacy D.Lgs. 196/03 e sicurezza sul lavoro D.Lgs. 81/08 (ex 626)

SAEV srl Via Ignazio Filone, 1 - Jesi (An) - 0731.21.56.39 - www.saev.biz - saev@saev.biz