



Associazione Italiana
Information Systems Auditors



AIEA FLASH

Ai nostri affezionati soci

Si sta chiudendo l'anno 2007 e ti ringraziamo di averci sostenuto. Alla data, tu sei uno dei **639 iscritti** all'Associazione. Speriamo che tu abbia avuto modo, come molti soci, di partecipare alle nostre iniziative (Sessioni di Studio, Convegno annuale, corsi...) ed apprezzare l'impegno di tutto il consiglio direttivo a venire incontro alle richieste dei soci.

Se tu non avessi potuto partecipare, ci sarebbe di aiuto conoscerne i motivi, in modo da proseguire nella ricerca del continuo miglioramento.

Per il 2008 stiamo programmando nuove iniziative, una maggiore offerta di corsi, una collaborazione ancor più importante con le Associazioni a noi vicine.

Siamo certi, quindi, che tu deciderai di rimanere nostro socio.

Le informazioni per il rinnovo della quota associativa sono sul sito dell'Associazione.

Per qualsiasi informazione, è a disposizione l'indirizzo di posta aiae@aiea.it

Aspettando il tuo rinnovo, il Consiglio Direttivo ringrazia ed **augura un Buon Natale**.

Parlano di noi

Sulla rivista Internal Audit di AIIA, nel numero di novembre, è uscita una intervista al nostro Presidente, Silvano Ongetta, sul tema "Obiettivo IT Governance". L'intervista completa sarà pubblicata nel prossimo numero di InfoAiea

Notizie dai Gruppi di Lavoro

Gruppo di lavoro "VAL-IT"

Il Gruppo di Lavoro "Traduzione VAL-IT" ha concluso i lavori. Il documento è stato stampato e sarà distribuito ai soci che parteciperanno alle prossime Sessioni di Studio.

Gruppo di lavoro "SOX2"

Il Gruppo di Lavoro "Sarbanes Oxley 2" ha concluso i lavori. Il documento originale è stato completamente tradotto ed è terminato anche il controllo qualità. Il documento sarà stampato e reso disponibile ai soci.

Esame CISA e CISM

Numerosi soci ci cimenteranno con l'esame CISA e CISM che si terrà sabato 8 dicembre. A tutti loro un grandissimo IN BOCCA AL LUPO!

Le prossime attività di AIEA

1. Per il quarto anno consecutivo, AIEA organizza a Lugano, in collaborazione con ATED, una Sessione di Studio sul tema IT Governance
2. Ricordiamo ai soci che è disponibile, sul sito www.aiea.it, il calendario aggiornato di tutti gli eventi e dei corsi programmati nel prossimo anno.



Il prossimo Convegno annuale

Tutto il Consiglio Direttivo, al quale si affiancano alcuni soci, sta lavorando all'organizzazione del prossimo Convegno. Prevediamo che si terrà nella seconda quindicina del mese di maggio 2008, probabilmente in una città dell'Emilia. Vi terremo informati.

Notizie da ISACA

Riceviamo da ISACA:

At the upcoming International Conference, ISACA will formally announce its newest credential program specifically developed for professionals who have responsibilities for managing and/or governing the IT-related contribution to an enterprise to achieve its business objectives. The certification, supported by the IT Governance Institute® (ITGEIT) and built on its intellectual property, will promote the advancement of IT professionals who wish to be recognized for their governance-related experience and knowledge. The formal name of the certification is expected to be announced shortly, at which time an announcement will be available at www.isaca.org/news.

The initial IT governance professional certification exam is expected to be administered in December 2008. A grandfathering program will be announced shortly, through which highly experienced IT governance professionals may apply for certification without taking the exam. More information will be available soon on the ISACA and ITGI web sites, www.isaca.org and www.itgi.org.

Member Benefit of the Month

COBIT 4.1:

1: ISACA members have access to a complimentary download of COBIT® 4.1, as well as to certain COBIT-related documents including IT Assurance Guide: Using COBIT® and its appendices in Excel, IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition, and the content of its accompanying IT Governance Implementation Guide—Supplemental Tools and Materials CD-ROM. Members can also browse most areas of COBIT Online®.

2: Available at www.isaca.org/downloads

Chapter size

Because of the extensive growth of the association and its chapters, the Membership Board has adjusted the official chapter size categories used for awards judging. The new size categories are as follows:

Small: 100 members or less

Medium: 101-300 members

Large: 301-800 members

Very large: 801 or more members

Il sito AIEA

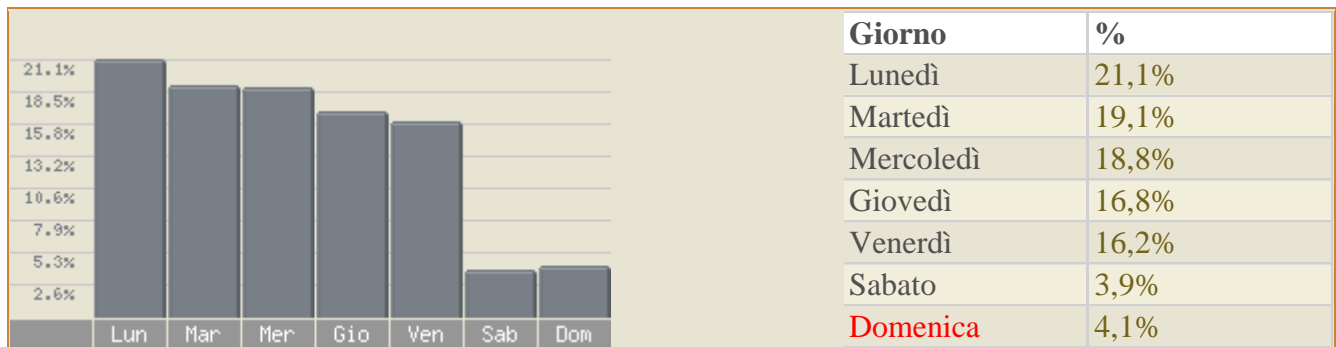
Continua la nostra lettura di chi, come e quando, accede al nostro sito.

Di seguito la percentuale dei paesi di provenienza, sul totale degli accessi di novembre:



■ Italia	84,17 %
■ Regno Unito	3,70 %
■ Svizzera	2,54 %
■ Germania	2,06 %
■ Unione Europea	1,23 %
■ Altri	6,31 %

E' interessante rilevare anche, come variano le visite, nei giorni della settimana. Nella settimana dal 5 all'11 novembre, l'andamento è stato il seguente:



Avviso ai soci

Per la stesura della Newsletter e per la predisposizione del notiziario InfoAIEA, stiamo cercando soci disposti a collaborare. L'idea è di mettere in piedi un "Comitato di redazione" che collabori alla messa a punto dei nostri due documenti. Chi fosse interessato è pregato rivolgersi in segreteria.

Partecipazione di soci ad eventi

Tutti i soci possono segnalare eventi, fatti e informazioni di possibile interesse comune da segnalare ad esempio nella newsletter.

In particolare, se partecipate ad un evento in qualità di organizzatore, relatore o simile, valutate la possibilità di partecipare a nome AIEA. La partecipazione dell'Associazione ad un evento "deve" però essere decisa dal Consiglio Direttivo: siete quindi pregati di contattare il CD con ragionevole anticipo!

Un saluto ad un amico che ci ha lasciati

Nello scorso mese di ottobre, dopo lunga malattia, ci ha lasciati il nostro socio ed amico Giorgio Gallina (TI Audit and Compliance Services SCARL) Ai familiari e ai colleghi giungano le nostre più sentite condoglianze.

Bibliografia

E' on line il nuovo numero di InterLex (<http://www.interlex.it>)

Vi informiamo che sul sito www.cnipa.it sono disponibili molti documenti di interesse per i nostri soci. Ricordiamo, inoltre, che il CNIPA organizza incontri o seminari aperti anche ai soci AIEA.



ESTRATTO NEWSLETTER CLUSIT

30 novembre 2007 - Newsletter CLUSIT - www.clusit.it
disponibile in PDF all'indirizzo www.clusit.it/newsletter_30_11_07.pdf

=====

LA SICUREZZA DELLE PMI AL CENTRO DELL'ATTENZIONE DEL CONVEGNO ENISA A BARCELLONA

=====

Il CLUSIT è stato presente al convegno "Information Risk Management: Why Business Need It? " organizzato a Barcellona nei giorni 8 e 9 Novembre dall'agenzia europea ENISA e dall'Istituto Nacional de Tecnologías della Comunicaciòn. Il convegno, estremamente interessante e concreto, ha affrontato da diverse prospettive il problema del risk management in azienda, in particolare con una forte attenzione alle esigenze ed alle difficoltà delle PMI e delle microimprese. Sono state portate le esperienze di diverse iniziative svoltesi in Spagna, Francia, Regno Unito, Germania e Austria. Le iniziative sono state promosse da diverse organizzazioni, dalle Pubbliche Amministrazioni Centrali fino alle Camere di Commercio e alle associazioni professionali.

Il convegno è stato occasione per il CLUSIT per stabilire contatti con lo scopo di acquisire le esperienze di queste organizzazioni per contribuire ad affrontare, anche in Italia, le difficoltà che hanno le PMI e microimprese nel gestire le problematiche di rischio e di sicurezza IT.

Nel complesso, dalle esperienze presentate emerge che un punto fondamentale è capire il linguaggio da utilizzare con le PMI, dove con PMI non si intendono i loro tecnici ma i loro manager. La situazione per cui le PMI e in particolare le microimprese non hanno personale competente interno è comune a tutta l'Europa. È necessario quindi affrontare i problemi dal punto di vista del business dell'azienda e non dell'IT; la protezione del sistema informativo deve risultare come conseguenza della protezione delle attività aziendali. Le presentazioni sono state infatti focalizzate sulla protezione dell'operatività dell'azienda; solo marginalmente sono state citate ad esempio le problematiche di compliance, ma mai come scopo trainante delle attività.

È stato anche affrontato il problema di come offrire degli strumenti semplificati, adatti al contesto specifico delle PMI.

Di particolare interesse è stata la presentazione dell'iniziativa della Camera di Commercio austriaca IT-Safe (<http://it-safe.at>).

L'iniziativa comprende dei manuali ben focalizzati sulle PMI, non rivolti al personale IT ma a dirigenti e dipendenti. Prevede inoltre un questionario di autovalutazione (scelta molto comune come approccio, aiuta la PMI a ragionare sui propri problemi) in base al quale vengono forniti i "capitoli interessanti" dei manuali. Infine, l'iniziativa comprende un servizio di consulenza, pagato ad ore dalle PMI, per attività di audit e advising, anche questa rivolta ai manager dell'azienda, per permettere loro di capire quali sono i loro problemi e cosa chiedere ai propri fornitori.

Il CLUSIT sta valutando come mettere a frutto le esperienze acquisite, in particolare per avviare dei piloti con lo scopo di valutare quali siano gli strumenti più adatti per aiutare le PMI italiane a gestire il proprio rischio nell'ambito della sicurezza IT.

(Autore dell'articolo e referente per il Clusit: Claudio Telmon, membro del Comitato Direttivo)



IL COMITATO SCIENTIFICO

È Stato costituito il Comitato Scientifico per il 2008, che risulta composto da:

- **DANILO BRUSCHI**, Professore Ordinario di Informatica presso il Dipartimento di Informatica e Comunicazione dell'Università degli Studi di Milano, Presidente Onorario Clusit.
- **ANTONELLO Busetto**, Direttore dei Rapporti Istituzionali di Confindustria Servizi Innovativi e Tecnologici.
- **GIOVANNI BUTTARELLI**, Segretario Generale dell'Autorità Garante per la protezione dei dati personali.
- **MICHELE COLAJANNI**, Professore Ordinario presso il Dipartimento di Ingegneria dell'Informazione dell'Università degli Studi di Modena e Reggio Emilia.
- **BRUNO CRISPO**, Professore Associato presso il Dipartimento di Informatica e Telecomunicazioni dell'Università degli Studi di Trento.
- **ALFONSO FUGGETTA**, Amministratore Delegato e Direttore Scientifico del CEFRIEL.
- **LUIGI MANCINI**, Professore Ordinario di Informatica presso l'Università di Roma "La Sapienza".
- **CLAUDIO MANGANELLI**, Componente del CNIPA, è stato Presidente del Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle PA.
- **GIULIO OCCHINI**, Presidente uscente e Direttore Generale AICA (Associazione Italiana per l'Informatica ed il Calcolo Automatico).
- **SILVANO ONGETTA**, Presidente AIEA (Associazione Italiana Information Systems Auditors).
- **JOY MARINO**, VicePresidente AIIP (Associazione Italiana Internet Provider), Presidente della Commissione Regole del Registro ".IT" e membro del Comitato per l'Internet Governance Forum costituito dal Ministro Nicolais.
- **ERMINIO SEVESO**, Direttore Organizzazione e Sistemi di BTicino, Presidente AUSED (Associazione Utilizzatori Sistemi e tecnologie dell'Informazione).
- **DOMENICO VULPIANI**, Direttore del Servizio Polizia Postale e delle Comunicazioni. [in attesa di conferma]
- **GIOVANNI ZICCARDI**, Professore Associato di Informatica Giuridica e Informatica Giuridica Avanzata presso la Facoltà di Giurisprudenza dell'Università degli Studi di Milano.

I CONVEGNI

Nell'ambito della manifestazione di Milano (5-7 febbraio 2008), il Clusit ha organizzato 2 convegni, che prevedono ciascuno due relatori istituzionali di riferimento e la presentazione di case study da parte di alcune aziende.

6 Febbraio - Mattino - Convegno INFOSTORAGE

"Privacy: un'opportunità di crescita per le imprese e il paese"

La legge sulla privacy è stata di recente al centro di un intenso dibattito, partito dalla proposta di alcuni parlamentari di abolirne gli obblighi per le piccole imprese. Nell'ambito di questo convegno si ripercorreranno a ritroso alcuni degli eventi più significativi di questa vicenda, e si proporranno testimonianze di aziende che mostreranno come, a partire da tali obblighi previsti dalle legge sulla privacy, è stato possibile avviare, all'interno dell'azienda stessa, un percorso virtuoso per una protezione a 360° dei loro asset più critici.

Chairman: Danilo Bruschi, Presidente Onorario CLUSIT



Associazione Italiana
Information Systems Auditors



Relatori Istituzionali: Giovanni Buttarelli, Segretario Generale Autorità Garante per la protezione dei dati personali e Gianfranco Granara, Presidente CNA Comunicazione e Terziario Avanzato

6 Febbraio - Pomeriggio - Convegno INFOSTORAGE

"Sicurezza Informatica e Storage: l'evoluzione continua"

Sicurezza e storage sono sicuramente tra i settori che assorbono ed integrano a ritmi molto elevati le innovazioni tecnologiche e di processo che caratterizzano continuamente le information e communication technology. Anche gli esperti del settore riescono a fatica a tenere il passo dell'innovazione, per contro è estremamente importante per un'azienda riuscire a sfruttare il vantaggio competitivo che può essere offerto dai nuovi prodotti o servizi. In questo convegno cercheremo di delineare gli aspetti che caratterizzano i prodotti di ultima generazione nei due settori, e saranno presentati casi reali in cui gli stessi hanno contribuito a migliorare in diversi aspetti alcune realtà aziendali. Non mancherà uno sguardo ai trend evolutivi. Vedremo inoltre quali talenti e quali competenze sono necessarie per affrontare le nuove sfide della security.

Chairman: Umberto Torelli, Giornalista

Relatori istituzionali: Alfonso Fuggetta, Direttore Scientifico CEFRIEL e Gigi Tagliapietra, Presidente CLUSIT

LA FORMAZIONE

Abbiamo organizzato due seminari Clusit Education, seminari specialistici che danno diritto a crediti/ore CPE (Continuing Professional Education) validi per il mantenimento delle certificazioni CISSP, CSSP, CISA, CISM o analoghe richiedenti la formazione continua.

5 Febbraio - Pomeriggio

"Dal Penetration Testing alla Risk Analysis: la metodologia OSSTMM 3.0, lo standard ISO 27001 ed i punti di incontro"

Docenti: Raoul Chiesa e Fabio Guasconi

7 Febbraio - Mattino

(In fase di definizione)

IL PREMIO TESI

Il 7 febbraio, al pomeriggio, si svolgerà la premiazione della terza edizione del Premio Clusit "Innovare la sicurezza delle informazioni", che ogni anno ricompensa le migliori tesi universitarie sulla sicurezza delle informazioni.

Per informazioni sul Premio Clusit: <https://tesi.clusit.it/>, dove sono anche disponibili gli abstract delle tesi già presentate.

Rivolgiamo Un ringraziamento particolare agli sponsor dell'edizione 2008 del premio: BSI Management Systems, Emaze, Lampertz e @Mediaservice.net.



Associazione Italiana
Information Systems Auditors



NOTIZIE E SEGNALAZIONI DAI SOCI

È stato spostato al 20 dicembre il termine per la presentazione delle domande di iscrizione al Master di I livello in "Sicurezza dei sistemi e delle reti informatiche per l'impresa e la Pubblica Amministrazione" organizzato dal Dipartimento di Informatica dell'Università di Roma "La Sapienza". Per il bando ed ulteriori dettagli: <http://mastersicurezza.uniroma1.it/>

EVENTI SICUREZZA

13 dicembre 2007, Roma
Seminario Clusit
Programmazione Sicura
https://edu.clusit.it/scheda_seminario.php?id=15



ESTRATTO NEWSLETTER AIPSI Novembre 2007

In Primo Piano ##

Grande successo di pubblico ai seminari di e-Academy a SMAU 2007. In particolare, l'area sicurezza gestita da AIPSI ha organizzato 20 seminari, su tematiche che spaziano dalla crittografia quantistica all'informatica forense, dalla sicurezza del kernel a quella dei sistemi SCADA, frequentati con soddisfazione da centinaia di persone.

Ringraziamo tutti i relatori e tutti i visitatori che hanno contribuito al successo della manifestazione.

Attività dell'Associazione ##

- Certificazione LoCSI

Grazie al contributo di numerosi specialisti è ormai in dirittura d'arrivo la certificazione LoCSI. In questo anno sono stati fatti molti miglioramenti per adattare la certificazione alle esigenze del mercato e dei professionisti della sicurezza IT.

È stato definito un livello BASE della certificazione, destinato ai professionisti dell'IT che, pur occupandosi di sicurezza, non ne fanno l'oggetto principale della loro professione. Ne sono un esempio i gestori dei piccoli sistemi informativi delle PMI, che devono occuparsi di tutti gli aspetti della gestione dei loro sistemi, compresa la sicurezza. Anche per loro sarà possibile ottenere una certificazione che testimoni la loro preparazione sulle specificità del contesto italiano, ed in particolare della normativa.

È previsto un periodo di grandfathering, per semplificare l'accesso iniziale ai professionisti che da tempo operano nel settore della sicurezza IT e per favorire la diffusione della certificazione.

Stiamo inoltre predisponendo del materiale di studio più fruibile del mero elenco delle normative attualmente disponibile sul sito dell'associazione. Il materiale individua una selezione dei punti delle normative rilevanti per la certificazione, e le affronta in modo organico per temi. Il materiale sarà utilizzato per corsi di formazione che saranno erogati dall'inizio del 2008.

La qualificazione LoCSI sarà inquadrabile nello schema EUCIP sulle professionalità informatiche.

- AIPSI al Security Talk Show del 16 Novembre a Roma

Si è svolto a Roma l'evento "Information security tra legislazioni Locali e logiche multinazionali" con il patrocinio di AIPSI.

I soci De Paoli e Telmon hanno presentato la nostra iniziativa (con il supporto di C. Telmon) sulla certificazione AIPSI/LoCSI, suscitando notevole interesse, anche per i corsi di formazione. Si ringraziano Corrado Giustozzi di ZetaReticuli e Guido Pellillo di BAT per aver proposto ed organizzato l'evento insieme ad AIPSI.



- AIPSI ad OpenCON 2007 - Mestre, 30 Novembre

OpenCON è la prima ed l'unica conferenza europea gratuita interamente dedicata ad OpenBSD. L'evento si svolgerà a Mestre dal 30 Novembre al 2 Dicembre e vedrà Alessio L.R. Pennasilico tra i relatori.

Per maggiori informazioni visitate <http://www.opencon.org/>

- AIPSI a Infosecurity 2008 - Milano 5,6 e 7 Febbraio

AIPSI, già dallo scorso anno partner della manifestazione, partecipa ad Infosecurity con un proprio Stand e con un Corso di Forensic Analysis.

La manifestazione, che avrà luogo presso il Padiglione 17 della Fiera (il medesimo degli ultimi anni) si svolgerà nei giorni 5, 6 e 7 febbraio.

Il giorno 7 dalle ore 14:00 alle ore 17:00, AIPSI terrà un interessante Corso introduttivo di Forensic Analysis valido per accumulare Crediti (CPE).

Maggiori informazioni saranno reperibili sul sito

www.infosecurity.it e sul sito AIPSI www.aipsi.org

- AIPSI a eSecurity Lab 2008 - Milano 31 Gennaio 2008

Continua il patrocinio di AIPSI con la manifestazione e-Security LAB organizzata da BCI Italia con il supporto di AIPSI e altre associazioni quali CLUB-TI e FIDA Italia.

L'apertura dei lavori sarà a cura del presidente AIPSI con il keynote "Stato dell'arte e tendenze nelle soluzioni per la Sicurezza IT: scenario di mercato alla luce dell' approccio orientato al Risk Management".

L'evento si terrà il 31 Gennaio 2008 a Milano in una nuova location e avrà inizio alle ore 9:00.

Maggiori informazioni saranno reperibili sul sito

<http://www.bci-italia.com/> e www.aipsi.org

- Collaborazione con Assintel - Partecipazione di AIPSI al GDL (Gruppo di Lavoro) "Sicurezza per le PMI" con Assintel.

Gli obiettivi del progetto, per i quali saranno probabilmente disponibili dei finanziamenti per la sua realizzazione, sono riassumibili in:

- a.. Accrescimento della cultura in ambito sicurezza IT e Fisica per le PMI
- b.. Far comprendere l'importanza della sicurezza nelle PMI
- c.. Contribuire alla formazione necessaria per comprendere le normative di sicurezza che coinvolgono le PMI.

Il lavoro si concretizzerà nella realizzazione di "Quaderni" specifici per macro argomento trattato. E' prevista un'indagine a campione per meglio comprendere le necessità delle PMI e la promozione dell'iniziativa, attraverso convegni, presenza sui siti delle associazioni coinvolte (es. Assintel e AIPSI) e altro.

Gli argomenti sino ad oggi ipotizzati da considerare sono:

- a.. Analisi dei Rischi (lo richiede anche il Testo unico in materia di privacy: D.Lgs. 196/03)
- b.. Conservazione dei Dati (quando, come e perché conservarli)
- c.. Privacy (non c'è privacy senza sicurezza)
- d.. Back up (l'importanza di effettuare il backup e salvare i dati in un luogo sufficientemente distante dall'origine)
- e.. Business Continuity (come può un'azienda delle PMI "permettersi" un BCP)



- f.. Perdita dei dati (i dati si possono anche perdere ma è indispensabile poterli ricostruire: i dati elettronici sono ormai il patrimonio di ciascuno di noi!)
- g.. Identificazione/autenticazione (e' il concetto base per ogni azione che riguardi la sicurezza)
- h.. Firma Digitale
- i.. Furto d'identità
- j.. Internet
- k.. Posta elettronica

- Direttiva 2005/36 CE sul riconoscimento delle qualifiche professionali. Il Decreto Legge in recepimento della Direttiva UE in oggetto e' di imminente pubblicazione: AIPSI, in rappresentanza delle proprie professionalita' della Sicurezza Informatica, partecipa alle attivita' di avviamento del Forum sulle competenze digitali o relative all'ICMT (Information, Communication, Media Technology").

Eventi ##

- 5° Convegno Net&System Security 2007, Palazzo dei Congressi di Pisa:
analisi e vulnerabilità dei sistemi informatici.

L'evento nasce con il preciso scopo di creare un momento d'incontro tra le aree che caratterizzano il mondo dell'Informatica (Ricerca, Università, Studenti, Mondo del Lavoro, Tecnici) in cui sia possibile specialmente il confronto sulla sicurezza informatica, approfondendo le tematiche attuali, ed esaminando le ultime tecnologie.

Tema specifico di questo convegno sono le nuove frontiere dell' "IT-Security". I lavori occuperanno l'intera giornata durante la quale saranno approfonditi in modo particolare quegli aspetti che, nell'ultimo anno, si sono maggiormente imposti all'attenzione degli addetti ai lavori.

Saranno presenti numerosi relatori appartenenti ad AIPSI.

Info a questo link: <http://www.atsystemgroup.org/it/nss07>

- Nell'ottica di favorire la cultura della sicurezza informatica e nello spirito di collaborazione con le aziende e le associazioni, AIPSI partecipa ai seguenti eventi:

5 Dicembre ore 17:00 - CISO Forum AIPSI, insieme a CLUSIT e AIEA partecipano al CISO FORUM organizzato da CISCO "Opinioni a confronto sul futuro della Sicurezza", che si terrà a Milano il 5 dicembre 2007, alle ore 17.00, presso l'Hotel Hyatt, via Tommaso Grossi 1.

Moderatore del dibattito sarà Gigi Tagliapietra, Presidente di CLUSIT.

L'intervento sul tema Compliance sarà gestito da Silvano Ongetta, Presidente di AIEA, mentre la sessione sulla figura professionale del CISO sarà curata da Elio Molteni, Presidente di AIPSI.

ISSA News ##

- Submit Your Nominations Now for ISSA International Awards
Award categories include:



Associazione Italiana
Information Systems Auditors



1. Chapter Communication Program of the Year
2. Outstanding Information Security Professional of the Year
3. Outstanding Organization of the Year
4. Honor Roll
5. Outstanding Chapter of the Year

The 2007 Awards Committee invites chapters to submit nominations by Friday, November 30, 2007. Information on nominations available at www.issa.org/News/Events.html#ISSAawards.

- ISSA Webcast

I Webcast di ISSA sono disponibili su <http://www.issa.org/current-webcast.html> a partire dalla data indicata.



- PERIZIE TECNICHE, ACCESSO AI DATI E DIRITTO ALLA DIFESA
- PRIVACY E DIRITTI DEGLI UTENTI
- FILESHARING: DUBBI DELLA CORTE DI GIUSTIZIA DELL'UE

Perizie tecniche, accesso ai dati e diritto alla difesa

Non è possibile accedere alle perizie tecniche in presenza di un contenzioso

Non è possibile accedere alle perizie tecniche in presenza di un contenzioso, specie se queste contengono valutazioni che risultino indispensabili o quantomeno influenti nell'esercizio del diritto di difesa. Il Garante ha rigettato il ricorso di una persona che aveva avuto solo parziale risposta ad una richiesta di accesso rivolta ad una compagnia assicurativa. Il ricorrente chiedeva di conoscere i propri dati personali contenuti nelle copie integrali della perizia tecnica, comprese le valutazioni riservate del medico legale. La compagnia assicurativa da parte sua, opponendosi alla richiesta, sosteneva di aver fornito solo la parte "oggettiva" della documentazione richiesta, omettendo la parte conclusiva, per non ledere le proprie "esigenze difensive".

Nel definire il procedimento il Garante ha ribadito che va salvaguardato il diritto alla difesa delle parti e ha quindi riconosciuto le ragioni all'assicurazione di differire l'accesso del ricorrente. E ciò non soltanto per l'esistenza di un giudizio civile pendente, ma anche perché si era in presenza di una specifica situazione che avrebbe potuto condizionare o alterare l'esercizio del diritto di difesa dell'assicurazione. Il ricorrente infatti in un primo tempo aveva richiesto all'assicurazione un risarcimento per i danni materiali subiti e solo in un secondo momento aveva manifestato l'esigenza di un risarcimento per danni fisici, richiesta non accolta dalla compagnia assicurativa che aveva sollevato dei dubbi per la modesta entità dei danni prodotti dall'urto dei veicoli, con l'inevitabile ricorso ad una perizia medico legale.

Privacy e diritti degli utenti

Non si può utilizzare la legge sulla privacy per fini di tutela diversi da quelli della protezione dei dati personali.

Non si può utilizzare la legge sulla privacy per fini di tutela diversi da quelli della protezione dei dati personali. Lo ha ribadito il Garante in seguito al ricorso di numerosi utenti che contestavano l'utilizzo dei dati personali che li riguardavano da parte di un'azienda subentrata alla gestione comunale per la fornitura del servizio idrico.

Gli utenti, sostenendo di non avere mai avviato un rapporto contrattuale con la società, contestavano il passaggio di gestione lamentando quindi un trattamento illegittimo dei dati personali. Pertanto continuavano a versare le somme derivanti dal consumo idrico su un conto corrente postale intestato al Comune, chiedendo all'azienda subentrata di interrompere l'invio di solleciti, comunicazioni e bollette. L'aumento delle tariffe operato dalla nuova società aveva causato una serie di rimostranze da parte degli utenti, che rivendicavano la gestione in economia operata in precedenza dall'ente locale. Gli interessati, dunque, hanno richiesto, prima alla società e poi al Garante, la cancellazione e il blocco dei dati che li riguardavano.

La società tuttavia, in seguito ad una serie di reclami pervenuti dopo l'invio delle prime fatture, aveva provveduto a inviare ai clienti lettere raccomandate, oltre a pubblicare su alcuni quotidiani locali una risposta cumulativa, in cui venivano fornite indicazioni in merito al trattamento dei dati personali, precisando che la loro cancellazione avrebbe comportato la risoluzione d'ufficio del contratto e, dunque, l'interruzione della fornitura del servizio idrico. Il Garante ha ritenuto infondato il ricorso poiché il passaggio di gestione è avvenuto in base a disposizioni di legge e il consenso degli utenti per il trattamento dei dati strettamente indispensabili all'erogazione e alla fatturazione del servizio non è richiesto, perché necessario per eseguire obblighi derivanti da un contratto di cui sono parte gli interessati.



- DIRITTO DI ACCESSO E DATI GENETICI
- GIORNALISTI: NO AD ARTIFICI NELLA RACCOLTA DELLE NOTIZIE
- I GARANTI DEL MONDO ALLA RICERCA DI REGOLE COMUNI

Diritto di accesso e dati genetici

Non è in base alla legge sulla privacy che si possono intraprendere azioni per ottenere campioni biologici sui quali eseguire poi un'indagine genetica. Avvalendosi del diritto di accesso riconosciuto dal Codice privacy si possono infatti conoscere i dati genetici, anche di un defunto, solo se riportati in referti, cartelle cliniche ecc. Ciò non esclude comunque che la persona interessata non possa esercitare altre azioni nelle competenti sedi giudiziarie.

Lo ha stabilito il Garante definendo il ricorso di una donna che aveva richiesto, senza esito, ad una struttura sanitaria di entrare in possesso dei campioni biologici (frammenti di tessuto, prelievi ematici) del padre da poco deceduto. Lo scopo della signora era quello di eseguire un'analisi genetica per poter avere certezze sulla propria origine, senza esercitare azioni di disconoscimento di paternità.

Il ricorso è stato ritenuto inammissibile, perché avviato senza una effettiva richiesta di accesso ai dati.

L'Autorità ha comunque precisato che le informazioni genotipiche caratteristiche di un individuo, contenute in ogni campione di materiale biologico, assumono il carattere di dati personali, e diventano suscettibili di tutti i diritti di cui all'articolo 7 del Codice, solo se sono estrapolate dal campione biologico e conservate dal titolare, in questo caso dall'ospedale, in referti, cartelle cliniche ecc..

Alla signora non viene tuttavia preclusa la possibilità di formulare eventuali altre legittime richieste di accesso a dati personali effettivamente esistenti, già estrapolati e archiviati, o di attivare altre procedure di fronte al giudice ordinario per tutelare i suoi diritti.

Giornalisti: no ad artifici nella raccolta delle notizie

Un giornalista non può usare "artifici" per svolgere la sua attività, e deve rendere nota la sua professione a

meno che vi siano rischi per la propria incolumità o non possa, altrimenti, adempiere alla funzione informativa. E' illecito, quindi, utilizzare per un servizio giornalistico brani di conversazioni ed immagini di colloqui privati ripresi con una telecamera nascosta senza che vi siano fondati motivi. Per questo il Garante ha ordinato ad una televisione via satellite di non trasmettere più un servizio giornalistico e di cancellarlo dal proprio sito Internet. Accogliendo i ricorsi di tre imam, ai quali si erano rivolti due giornalisti fingendosi coniugi di fede musulmana alla ricerca di un consulto religioso, il Garante ha ritenuto che siano stati violati i principi sulla protezione dei dati personali e del codice deontologico in materia di giornalismo. E in particolare quelli relativi all'obbligo del giornalista di rendere note le finalità di un colloquio - ossia di star raccogliendo informazioni per un servizio giornalistico - e di evitare l'uso di "artifici". Pur sussistendo, infatti, l'interesse pubblico a conoscere le opinioni delle guide religiose di alcune delle principali moschee italiane sull'uso del velo da parte delle donne, dalla ricostruzione dei fatti è emerso che i giornalisti non hanno informato gli imam né dell'uso della telecamera, né che le loro dichiarazioni sarebbero state utilizzate per un servizio giornalistico. Non pertinenti e non essenziali all'informazione sono risultate, inoltre, le traduzioni di brani di telefonate ricevute da uno degli imam durante i colloqui e riportate nel servizio. Non ricorreva, poi, sempre secondo l'Autorità, un'ipotesi prevista dal codice deontologico alla quale si appellava invece la società televisiva che consente al "giornalista che raccoglie notizie" di non qualificarsi solo nel caso in cui "ciò comporti rischi per la sua incolumità o renda altrimenti impossibile l'esercizio della funzione informativa". I due giornalisti televisivi, infatti, avevano reso nota, seppure genericamente, la propria professione agli imam che li avevano comunque ammessi nei loro uffici

all'interno delle moschee ed avevano continuato a fornire informazioni, anche se gli stessi le annotavano su un taccuino.

In conseguenza dell'illecita raccolta dei dati il Garante ha vietato anche ad un quotidiano l'ulteriore diffusione sul proprio sito delle informazioni relative ai due imam, in particolare le loro immagini, pubblicate in un articolo in cui si anticipava la messa in onda del servizio.

I Garanti del mondo alla ricerca di regole comuni

Tra le risoluzioni approvate a Montreal anche quella sulla necessità di tradurre in standard tecnologici i principi di protezione dei dati

Tre importanti risoluzioni sono state adottate dalla Conferenza internazionale che ha visto riunite a Montreal, dal 25 al 28 settembre, tutte le Autorità di protezione dati a livello mondiale. La Conferenza, intitolata "Terra Incognita – Gli orizzonti della protezione dei dati", ha affrontato le grandi sfide dei nostri anni e di quelli a venire: sicurezza e globalizzazione, rischi e potenzialità della Rete, nuove tecnologie e tracciamento delle persone, dati genetici e bio-banche.

La prima delle tre risoluzioni approvate sottolinea l'urgenza di pervenire a criteri condivisi a livello mondiale per tutelare i dati dei passeggeri, oggetto di pressioni sempre più forti da parte dei Governi di molti Paesi del mondo. La natura del problema richiede soluzioni globali e i Garanti chiedono a tutte le parti in causa (soggetti pubblici e privati, Ong, Autorità di protezione dati) di collaborare per garantire alcuni principi basilari comuni rispetto alla raccolta ed all'utilizzazione di questi dati. L'obiettivo è quello di conciliare le esigenze connesse alla lotta al terrorismo con la tutela dei diritti dei cittadini e delle imprese coinvolte. I principi riguardano la trasparenza nelle finalità della raccolta dei dati; la loro utilizzazione soltanto quando realmente indispensabili; il rispetto di criteri di proporzionalità nella raccolta; i limiti al numero dei soggetti ai quali possono essere comunicati; l'accuratezza delle informazioni; le garanzie per i cittadini che intendano esercitare diritti di accesso o rettifica dei dati stessi, ad iniziare da un'adeguata informativa rispetto all'intero trattamento ed alle sue caratteristiche.

Una seconda risoluzione affronta il problema della definizione di standard universali in materia di privacy in collaborazione con l'Iso (l'organismo internazionale che si occupa di fissare standard tecnologici e di processo). Il tentativo di tradurre i principi di protezione dati in regole tecnologicamente efficaci merita di essere sostenuto, anche se attualmente in ambito Iso ciò avviene con riguardo soprattutto alle

tematiche della sicurezza dei sistemi informativi più che alle metodologie per garantire il rispetto della privacy. La Conferenza di Montreal invita tutte le Autorità di protezione dati a partecipare attivamente al processo di definizione di tali standard anche attraverso un migliore coordinamento delle iniziative nazionali ed il coinvolgimento diffuso del mondo scientifico e della ricerca.

La terza risoluzione è dedicata all'esigenza di potenziare la cooperazione internazionale ricercando convergenze con altri organismi (quali l'Ocse, il Consiglio d'Europa, l'Apec) che stanno sviluppando, in maniera diversa ed a livelli diversi, strumenti a sostegno della protezione dei dati e della privacy, nel solco delle indicazioni fornite dalla Conferenza internazionale delle autorità tenutasi nel 2006 a Londra.

Filesharing: dubbi della Corte di giustizia dell'Ue

Un elemento importante si è aggiunto di recente al dibattito in corso sulla legittimità delle richieste che varie società discografiche e di altri settori stanno avanzando alle autorità giudiziarie di più Paesi europei per costringere gli Internet provider a comunicare loro i nominativi degli utenti associati agli indirizzi Ip che risultano coinvolti in attività di filesharing (condivisione di file, in particolare musicali o video, basata sul sistema detto peer-to-peer), a causa della presunta violazione del copyright associata a tali attività.

Si tratta delle conclusioni dell'avvocato generale Juliane Kokott relative ad un caso attualmente all'esame della Corte di giustizia dell'Ue (causa n. C-275/06 in <http://curia.europa.eu>) che vede un'associazione spagnola di produttori musicali (Promusicae) opposta al principale gestore telefonico spagnolo (Telefónica). Le conclusioni chiariscono che le disposizioni del diritto comunitario in materia di protezione dei dati nelle comunicazioni elettroniche permettono di trasmettere i dati sul traffico delle comunicazioni personali soltanto alle competenti autorità statali, e non direttamente ai titolari di diritti d'autore che intendano far valere in sede civile la violazione dei loro diritti.

In altri termini, nessuna direttiva europea in materia di comunicazioni elettroniche consente di comunicare a soggetti privati dati relativi al traffico delle comunicazioni, se non in presenza di gravi e circostanziati motivi quali il fatto che la violazione del copyright sia commessa a scopo di lucro, e quindi in modo da pregiudicare gravemente gli interessi economici del titolare del diritto.

Neppure la direttiva 2006/24, sulla cosiddetta "data retention", che prevede l'obbligo per i fornitori di servizi di comunicazioni elettroniche accessibili al pubblico di conservare comunque una serie di dati di traffico, consente questo tipo di comunicazioni. Tuttavia, tale conservazione è finalizzata all'indagine, all'accertamento ed al perseguimento di reati gravi e i dati in questione possono dunque essere trasmessi soltanto alle autorità nazionali competenti.

Si attende ancora il pronunciamento della Corte di giustizia sul caso, ma la posizione dell'Avvocato generale sembra allinearsi a quella di varie Autorità per la protezione dei dati di Paesi europei. Sul punto è in corso un articolato dibattito che coinvolge, a vari livelli ed in più sedi internazionali, i soggetti interessati. Recentemente, inoltre, vi sono state alcune decisioni di autorità giudiziarie tedesche (Offenburg, Hanover, Berlino) che hanno respinto le richieste di accesso ai dati Ip formulate da varie società discografiche con motivazioni molto simili a quelle utilizzate nelle conclusioni del giudice Kokott.

Come indicato dall'Avvocato generale, il legislatore comunitario ha sempre fatto salve le disposizioni in materia di tutela dei dati personali (sia nella direttiva sul commercio elettronico, 2000/31, sia in quella sulla tutela della proprietà intellettuale, 2004/48), e "non ha ritenuto opportuno limitare la tutela dei dati personali a favore di una tutela della proprietà intellettuale".



- CALL CENTER: ARRIVANO LE SANZIONI DEL GARANTE
- I GIORNALISTI GARANTISCONO AI MINORI TUTELE EFFETTIVE
- IMMIGRAZIONE CLANDESTINA: DATI DEI PASSEGGERI AEREI NEL RISPETTO DELLA PRIVACY

Call center: arrivano le sanzioni del Garante

Per servizi non richiesti e telefonate indesiderate 60 sanzioni per oltre 260 mila euro ai gestori telefonici

Sessanta sanzioni applicate e oltre 260 mila euro già versati sono solo i primi risultati dei recenti interventi del Garante sull'operato dei call center a tutela degli utenti telefonici. Le sanzioni comminate a gestori di telefonia fissa e mobile per illeciti trattamenti di dati personali riguardano prevalentemente attivazione di servizi non richiesti (cambi di operatore, linee Internet veloci, servizi aggiuntivi) e, in misura minore, telefonate pubblicitarie indesiderate. Le società telefoniche hanno preferito, in molti casi, chiudere subito il contenzioso attraverso il pagamento anticipato in misura ridotta, previsto per chi non intenda impugnare la contestazione della violazione.

Prosegue in questo modo l'azione del Garante a tutela degli utenti telefonici che numerosi segnalano costi e disagi derivanti da un uso scorretto dei loro dati personali da parte dei call center dei principali gestori (Telecom, Tele2, Fastweb, Wind, Eutelia, Tiscali). Nella maggior parte dei casi è stato sufficiente che chiunque, un figlio, un collaboratore di famiglia, rispondesse al telefono e senza dare alcun assenso a quanto veniva proposto, perché venissero attivati servizi mai richiesti con conseguenti fatturazioni di costi in bolletta, distacco, anche per alcuni mesi, della linea telefonica, attese per il passaggio ad un altro operatore. A volte non c'è stata neanche la telefonata e l'utente si è accorto di "aver aderito" a qualche nuova offerta solo al ricevimento della bolletta.

Le sanzioni sono frutto dell'applicazione da parte del Garante del provvedimento generale dello scorso anno cui avevano fatto seguito cinque specifici provvedimenti lo scorso giugno, con i quali aveva imposto a gestori e call center di interrompere comportamenti illeciti di dati. L'Autorità ha infatti effettuato una serie di ispezioni presso i call center, sia interni sia esterni, di cui si servono i principali gestori telefonici: dalle verifiche è emerso

che la maggior parte dei call center non informavano adeguatamente le persone contattate o operavano addirittura senza dire all'utente che si stavano raccogliendo i suoi dati, per quali finalità venivano usati, se era obbligato o meno a comunicarli, quali erano i suoi diritti. I call center hanno invece l'obbligo di informare con la massima trasparenza gli utenti sulla provenienza dei dati e sul loro uso e, se richiesto, di registrare la volontà dell'abbonato di non essere più disturbato. Per omessa o inidonea informativa il Codice privacy prevede una sanzione che va da 3000 a 18.000 euro, che può essere aumentata sino al triplo a seconda delle condizioni economiche della società.

I giornalisti garantiscono ai minori tutele effettive

Non basta omettere il cognome per tutelare un minore, anche i riferimenti indiretti lo rendono identificabile

Non basta omettere il cognome per tutelare un minore, se poi nell'articolo giornalistico vengono forniti particolari tali da renderlo facilmente identificabile. E' quanto ha ribadito il Garante (relatore Mauro Paissan) nell'accogliere il ricorso di una donna che riteneva di aver subito una violazione dei propri dati personali e di quelli dei propri figli da parte di un quotidiano. La vicenda si riferisce ad un fatto di cronaca nel quale era coinvolto un bambino che, conteso dai genitori separati, era poi stato ricoverato in ospedale. Motivo del ricorso della donna non era tanto il fatto in sé quanto quello che nell'articolo, pur non essendo citati il cognome degli interessati, venivano forniti numerosi particolari che avrebbero facilmente permesso l'identificazione dei soggetti: città in cui si è svolta la vicenda, nome, età e particolari dettagliati sulla salute del minore, nome ed età della sorella (pure minore), nomi ed iniziali del cognome dei genitori, loro professione, luogo di attuale residenza della madre. Molti, dunque, gli elementi forniti dal giornalista sulla base dei quali sarebbe stato possibile, ad un numero significativo di persone, riconoscere la ricorrente e i suoi due figli.

Il Garante ha ribadito che, anche quando si ricorre all'oscuramento dei nomi, se si forniscono dettagli tali da poter identificare la persona oggetto del fatto di cronaca si lede il suo diritto alla privacy, circostanza ancora più grave se si tratta di un minore.

Il Garante ha invece rigettato la seconda parte dell'istanza della ricorrente, nella quale si chiedeva la cancellazione dall'archivio del quotidiano delle informazioni relative ai protagonisti della vicenda e di poter conoscere l'origine delle stesse: per quest'ultima richiesta, in particolare, l'Autorità ha ribadito che va rispettato il segreto professionale del giornalista. Il Garante ha quindi vietato al quotidiano l'ulteriore utilizzo dei dati in questione "quale misura necessaria a tutela dei diritti e delle libertà fondamentali degli interessati" e ha stabilito, a carico della società editrice del quotidiano, un risarcimento pari a 300 euro.

Immigrazione clandestina: dati dei passeggeri aerei nel rispetto della privacy

L'Italia ha recepito la direttiva comunitaria sull'obbligo per le compagnie aeree di comunicare alla polizia di frontiera i dati relativi ai passeggeri aerei

Con il decreto legislativo (144/2007), pubblicato in Gazzetta Ufficiale lo scorso 5 settembre, l'Italia ha recepito la direttiva comunitaria 2004/82 riguardante l'obbligo per i vettori aerei di comunicare alla polizia di frontiera i dati relativi alle persone trasportate (dati API – Advance Passenger Information). Nell'attività di recepimento si è tenuto conto dei rilievi formulati dall'Autorità in sede di lavori preparatori e il testo consente un bilanciamento tra protezione dei dati personali, tutela delle frontiere e lotta all'immigrazione clandestina.

Il decreto prevede l'obbligo per le compagnie aeree di comunicare alle autorità competenti in materia di controlli di polizia di frontiera, prima del termine del check-in, e solo su richiesta delle autorità stesse, alcuni dati relativi ai passeggeri: i dati corrispondono alle informazioni denominate "API" e sono specificati in misura tassativa. Il testo fissa poi alcune modalità relative alla raccolta, cancellazione e conservazione dei dati in oggetto. Va sottolineato che i dati API comprendono sostanzialmente le informazioni delle quali le compagnie aeree dispongono al momento del check-in (diversamente dai dati PNR, che riguardano, ad esempio, anche informazioni sulle modalità di pagamento, sull'assegnazione del posto, sulla natura di "frequent flyer" del passeggero, sui bagagli al seguito, ecc.)

Le osservazioni del Garante italiano, che hanno trovato riscontro nel decreto, si basavano in larga parte sulla

posizione assunta dall'Autorità nell'ambito del Gruppo dei Garanti europei a Bruxelles (Parere 9/2006 – WP127,

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp127_it.pdf).

Il Gruppo dei Garanti europei aveva ribadito, in primo luogo, la necessità che le norme nazionali di recepimento non prevedessero finalità ulteriori rispetto a quelle indicate nella direttiva per quanto concerne l'utilizzazione dei dati API – ossia, migliorare i controlli alle frontiere e combattere l'immigrazione illegale. Tale indicazione è stata rispettata nella norma italiana, ove si stabilisce chiaramente che lo scopo della raccolta consiste nel "migliorare i controlli alle frontiere e combattere l'immigrazione illegale" – in tal senso escludendo utilizzazioni ulteriori dei dati se non (come prevede l'art. 4) "a seguito di specifica segnalazione" per cui i dati si rendano "indispensabili" in relazione a finalità specifiche (prevenzione di pericoli per l'ordine pubblico, la sicurezza nazionale, o attività di indagine in corso). Inoltre, le attività di raccolta riguardano soltanto le persone trasportate "nel territorio italiano", si esclude cioè (secondo quanto indicato dal Gruppo Art. 29) la possibilità di estendere la raccolta ai dati di passeggeri su voli genericamente svolti all'interno dell'Unione europea.

Le osservazioni del Gruppo Articolo 29 si erano appuntate anche sulla necessità di limitare il periodo di conservazione dei dati. In questo senso il decreto prevede che i dati richiesti dovranno essere comunicati dalle compagnie aeree per via telematica alle competenti autorità, le quali li registrano "in via provvisoria" provvedendo a cancellarli entro 24 ore qualora non risultino "necessari" per il contrasto dell'immigrazione illegale. I dati che invece risultino necessari a tale scopo, nei termini sopra indicati, potranno essere conservati per non oltre sei mesi. Anche le compagnie aeree sono tenute a cancellare i dati da esse comunicati, entro 24 ore dall'arrivo del volo.

Netta delimitazione poi delle categorie di dati oggetto di comunicazione. Si tratta delle sole categorie indicate nella direttiva, che pure sembrava lasciare agli Stati membri un certo margine di manovra rispetto all'inclusione di dati ulteriori (ad esempio, biometrici). Restano fermi, inoltre, gli obblighi di informare i passeggeri ai sensi del Codice privacy e di osservare ogni altra disposizione sul trattamento dei dati; in particolare, si fa specificamente menzione del rispetto dei principi di proporzionalità, finalità e conservazione limitata nel tempo.

Un decreto interministeriale che dovrà essere adottato entro il 20 dicembre 2007 (con il parere favorevole del Garante) definirà le modalità tecniche ed operative per la comunicazione dei dati API (anche con riguardo alle idonee misure di sicurezza). Il Garante vigilerà sull'attuazione del decreto e sull'effettivo rispetto delle misure a tutela della riservatezza in esso previste.

NEWSLETTER

del Garante per la protezione dei dati personali
(Reg. al Trib. di Roma n.258 del 7/6/99).
Direttore responsabile: Baldo Meo.

Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n.121 - 00186 Roma.
Tel: 06/69677751 - Fax: 06/69677755. Newsletter è consultabile sul sito Internet www.garanteprivacy.it



- “TELECAMERE CON VISTA”
- NO ALLA VOCE “PIGNORAMENTO” SUL CEDOLINO DELLA PENSIONE
- MEDIA E SPORT: REGOLE PER CHI TELEFONA IN TRASMISSIONE

“Telecamere con vista”

Il Garante interviene nei confronti di un Comune

Garantire la sicurezza di un quartiere non giustifica la presenza di telecamere che, anche in modo occasionale e involontario, riprendano interni di abitazioni private, violando in questo modo la privacy dei cittadini che vi risiedono. E’ quanto stabilito dal Garante Privacy nel provvedimento (relatore Mauro Paissan) sulla segnalazione di un cittadino che riteneva leso il proprio diritto alla riservatezza dalla presenza di diverse telecamere installate dal comune in prossimità del proprio stabile e in grado di “guardare” fin all’interno delle abitazioni. Le telecamere, come dichiarato dal comune, erano state posizionate, oltre che per monitorare il traffico, anche per esigenze di maggiore sicurezza dei cittadini, tutela del patrimonio e controllo di determinate aree. In un primo momento il comune aveva comunicato che l’impianto era programmato in modo da non riprendere edifici privati ed era comunque in grado, attraverso un sistema di mascheratura dinamica delle finestre, eventualmente riprese, di garantire la riservatezza delle persone. Tuttavia dopo aver visionato alcune foto presentate dal ricorrente, l’Autorità ha disposto un sopralluogo dal quale è emerso che il tipo di telecamera installata (“Dome”) permette facilmente zoom, brandeggio e identificazione dei tratti somatici delle persone che vengono riprese. Pur non essendo posizionate in direzione delle abitazioni, il sistema consente a qualsiasi operatore, che abbia accesso diretto al server, di spostare le telecamere nelle diverse angolazioni e operare così un’intromissione ingiustificata nella vita privata degli interessati. Valutati questi elementi il Garante ha stabilito che, per utilizzare lecitamente il sistema di videosorveglianza, il comune deve adottare ogni accorgimento volto ad evitare la ripresa di persone in abitazioni private; dovrà delimitare, quindi, la dislocazione, l’uso dello zoom e, in particolare, l’angolo visuale delle telecamere in modo da escludere ogni forma di ripresa, anche quando non c’è registrazione, di spazi interni di abitazioni private, attraverso eventuali sistemi di settaggio e oscuramento automatico, non modificabili dall’operatore. Il comune dovrà integrare inoltre il modello di informativa

indicando, oltre al monitoraggio del traffico, le finalità di sicurezza e di controllo di sua competenza.

No alla voce “pignoramento” sul cedolino della pensione

Si devono usare formule generiche o codici

Non si può utilizzare la dicitura “pignoramento” sul cedolino della pensione. Si devono utilizzare altre espressioni più rispettose della riservatezza della persona, come formule generiche o codici identificativi. Lo ha affermato il Garante Privacy accogliendo il ricorso di un pensionato, invalido civile, che si è opposto all’uso da parte dell’ente previdenziale della dicitura “pignoramento” sul cedolino della pensione per indicare una trattenuta che gli veniva operata. L’interessato ha chiesto la sostituzione con espressioni più generiche, tali da non consentire a terzi di venire immediatamente a conoscenza di delicati aspetti della propria sfera privata. Ciò, anche in considerazione del fatto che i cedolini della pensione, essendo spesso presentati per permettere acquisti con agevolazioni fiscali o per richiedere mutui e finanziamenti, possono circolare tra più persone. Dal canto suo l’istituto di previdenza ha fatto presente che il cedolino della pensione riportava genericamente l’esistenza di una trattenuta per pignoramento senza indicare però la causa (ad esempio per alimenti, tasse o altro); riteneva poi tale riferimento congruo, consentendo proprio ai terzi di valutare la reale situazione patrimoniale e la porzione disponibile della pensione. L’istituto si è reso comunque disponibile a utilizzare un’altra formula priva della parola “pignoramento”. Nell’accogliere il ricorso, il Garante ha richiamato il rispetto del principio di pertinenza e non eccedenza: pur ritenendo lecito l’uso di dati necessari a documentare le diverse voci relative alle competenze e alle trattenute in modo tale da consentire al pensionato di verificare l’esattezza della retribuzione, l’Autorità ha affermato che le finalità di documentazione e di trasparenza possono essere perseguite con metodi che, pur permettendo di individuare l’esistenza della ritenuta, non la descriva nel dettaglio: ad esempio, mediante l’utilizzo di

diciture meno specifiche (“trattenute presso terzi”, “recupero obbligatorio”) oppure di codici identificativi. All’ente che dovrà dare conferma all’Autorità dell’avvenuto adempimento sono state imputate le spese del procedimento.

Media e sport: regole per chi telefona in trasmissione

Il Garante per la protezione dei dati personali ha espresso parere favorevole sullo schema di decreto del Ministero delle comunicazioni che recepisce il “codice media e sport” di autoregolamentazione dell’informazione sportiva. Con il codice, il Ministero intende contribuire alla diffusione dei valori dello sport per contrastare fenomeni di violenza legati allo svolgimento di manifestazioni sportive, in particolare, di quelle calcistiche. Il Garante ha rivolto in particolare la sua attenzione sull’articolo 3, del codice in base al quale emittenti e fornitori di contenuti si impegnano a realizzare misure adatte, quando necessario, a rendere individuabili le persone che si collegano telefonicamente, in audio o in audio video, alle trasmissioni. Il Garante ha ritenuto questa previsione coerente rispetto alle finalità perseguite dal “codice media e sport”, sia per la sua valenza dissuasiva (in caso di telefonate che incitano alla violenza), sia per l’aiuto che esso può fornire alle emittenti alle quali spetta il compito di valutare l’idoneità a partecipare ad ulteriori trasmissioni di quei soggetti che si sono resi responsabili di violazione del codice di autoregolamentazione. Il Garante ha indicato alcune ipotesi che il Ministero, una volta recepito il codice, potrà eventualmente valutare per uniformare i comportamenti delle emittenti riguardo alle misure da adottare: annotazione del numero telefonico o a seconda dei casi richiesta delle generalità del chiamante; tempi di conservazione dei dati quando non si sono verificate violazioni del codice. Al codice di autoregolamentazione hanno aderito, tra gli altri, emittenti televisive e radiofoniche, l’Ordine dei giornalisti, l’Unione stampa sportiva italiana la Fnsi, la Fieg.

L’attività del Garante. Per chi vuole saperne di più

Gli interventi e i provvedimenti più importanti recentemente adottati dall’Autorità

- Linee guida sul trattamento dei dati personali della clientela in ambito bancario – Comunicato del 28.11.2007

- “Dalla parte del paziente”: il nuovo opuscolo divulgativo del Garante – Comunicato del 15.11.2007

- Indagine di Perugia. Il Garante richiama i media al rispetto della dignità della vittima – Comunicato del 10.11.2007

- Diffusione dati sui redditi sì, ma nel rispetto delle leggi – Comunicato del 9.11.2007

NEWSLETTER

del Garante per la protezione dei dati personali
(Reg. al Trib. di Roma n.258 del 7/6/99).
Direttore responsabile: Baldo Meo.

Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n.121 - 00186 Roma.
Tel: 06/69677751 - Fax: 06/69677755. Newsletter è consultabile sul sito Internet www.garanteprivacy.it