



---

Associazione Italiana  
Information Systems Auditors

---



## **Il XXII Convegno AIEA e altro.....**

Siamo arrivati al convegno. Sì, eccoci pronti ad accogliere i soci a Parma, per condividere esperienze ed indicazioni dai relatori, ma anche dai colleghi che incontreremo.

Anche quest'anno, abbiamo aperto una finestra fuori dall'Italia, per vedere e verificare cosa viene fatto oltrelpe. Riteniamo, infatti, determinante, aprirci al confronto con colleghi stranieri e, con loro, capire come si sta evolvendo il nostro ruolo.

Sul sito è presente la locandina e potrete trovare tutte le informazioni e le fasce di sconti sulle quote di iscrizione.

Vi aspettiamo!

## **Gruppi di ricerca**

### ***Gruppo di Ricerca "COBIT 4.1 - Iso 27001"***

E' terminata la stampa del documento: sarà la nostra quarta Guida della collana, che distribuiremo al Convegno. Un ringraziamento ai componenti del gruppo:

Fabrizio Cirilli (ISMS IUG Italian Charter) e Alberto Piamonte (Gruppo Adfor SpA), coordinati da Mario Notari (SEP Servizi e Progetti SpA)

### ***Gruppo di Lavoro "Traduzione COBIT 4.1"***

Dopo la diffusione del primo dominio, ME, che è disponibile sul sito (area Downloads), sono in corso sia il controllo qualità sia l'editing finale degli altri domini. Si prevede di rilasciare a breve il dominio "Erogazione e Assistenza

### ***Gruppo di Lavoro "Business Continuity"***

E' in corso il controllo qualità del documento finale. Si prevede che venga rilasciato entro il prossimo mese di luglio.

## **I soci partecipano**

Il socio Stefano Niccolini ha partecipato come relatore al Seminario del 29/4/08 - "Information Technology & Security Aziendale" - Camera Commercio di Milano

Parteciperà come "socio AIEA"



## Calendario Eventi AIEA

### Maggio

2-31 .....Milano – Roma proseguono i corsi CISA e CISM

### Giugno

5/6 .....Parma – Convegno Nazionale

### Luglio

24 .....Milano – Assemblea soci

## I prossimi eventi di AIEA

### Notizie da ISACA 1

Riceviamo da ISACA:

### Member Benefit of the Month: K-NET

K-NET is an online knowledge base consisting of more than 6,000 peer-reviewed electronic resources, organized by professional topic category and accessible by members only. Push technology allows members to be advised via e-mail when new content is added to their selected areas of professional interest. K-NET is available at [www.isaca.org/knet](http://www.isaca.org/knet).

### ISACA Benefit of the Month

Following the highly successful IT Control Objectives for Sarbanes-Oxley, ITGI presents IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance. This document provides a framework for managing information risk in the context of Basel II. A free download of this publication is available to ISACA members at [www.isaca.org/downloads](http://www.isaca.org/downloads), and print copies can be purchased from the ISACA Bookstore at [www.isaca.org/bookstore](http://www.isaca.org/bookstore).

## Certification Update

### CISA CPE Policy Update

The CISA Certification Board has approved an update to the Certified Information Systems Auditor™ (CISA®) continuing professional education (CPE) policy. Performing peer reviews can now be counted as “contributions to the IS audit and control profession.” To view this addition and the full policy, please visit [www.isaca.org/cisacpepolicy](http://www.isaca.org/cisacpepolicy).

### CGEIT Certification Updates:

- Applications for Certified in the Governance grandfathering provision until 31 October general is available at [www.isaca.org/cgeit](http://www.isaca.org/cgeit).
- To date, more than 300 CGEIT grandfathering applications have been received.
- Registration for the first CGEIT exam, offered on 14 December 2008, will begin in mid-July.



of Enterprise IT™ (CGEIT™) are being accepted under the 2008. More information on this and the certification in



- To construct a quality exam, ISACA has elicited the support of IT governance professionals around the world. Exam items currently are being reviewed for the CGEIT exam. Those interested in supporting this effort may find additional information at [www.isaca.org/cgeititemwriter](http://www.isaca.org/cgeititemwriter).

Ricordiamo i prossimi eventi ISACA:

## Calendar of Events

Dates of conferences are indicated in **RED**; other dates and deadlines are indicated in **BLACK**.

### May

14 May..... Early-bird registration deadline for 2008  
International Conference

### June

5 June..... Early-bird registration deadline for Latin America  
CACS

9-13 June ..... **ISACA Training Week** Vancouver, British  
Columbia, Canada

14 June ..... CISA and CISM exam administration

19-20 June ..... **Sarbanes-Oxley Symposium** Rosemont, Illinois,  
USA

23-27 June..... **ISACA Training Week** Minneapolis, Minnesota,  
USA

25 June ..... Early-bird registration deadline for Information  
Security Management Conference and Network  
Security Conference in Las Vegas, Nevada, USA

## Notizie da ISACA 2

ISACA has just released the new **IT Assurance Framework (ITAF)** as its latest member benefit. To meet the need for clear guidance for IT controls, ISACA has created this comprehensive assurance model incorporating standards and best practices. ITAF provides a single source through which IT audit and assurance professionals can seek guidance, research policies and procedures, obtain audit and assurance programs, and develop effective reports. The framework also:

- Provides guidance on the design, conduct and reporting of IT audit and assurance assignments
- Defines terms and concepts specific to IT assurance
- Establishes standards, guidelines, and tools and techniques that address IT audit and assurance professional roles and responsibilities, knowledge and skills, diligence, conduct and reporting requirements.

The current version of ITAF incorporates ISACA's IS Auditing Standards and Guidelines and allows for new guidance to be properly indexed as it is developed and issued. It is designed to be a living document to enable relevant tools, techniques, white papers and publications to be placed with the framework.

ITAF is applicable to any formal audit or assessment engagement. Its design recognizes that IT assurance professionals are faced with different requirements and different types of audit and assurance assignments—ranging from leading an IT-focused audit to contributing to a financial or operational audit.

**ISACA is pleased to be able to offer ITAF to ISACA members as a complimentary PDF download from the ISACA web site.** It can be purchased by nonmembers for US \$45.



---

Associazione Italiana  
Information Systems Auditors

---



For further information or to download the publications, visit [www.isaca.org/itaf](http://www.isaca.org/itaf). Announcement of ITAF's availability will be sent to all ISACA members shortly.

### **AIEA e ANSSAIF**

Il nostro Presidente, Silvano Ongetta, è stato nominato proboviro di ANSSAIF. Nella Newsletter di ANSSAIF, allegata, viene riportato l'annuncio ufficiale.

### **I soci AIEA sono invitati.....**

Da itSMF riceviamo questa comunicazione:

*"L'evento di Primavera 2008 di itSMF Italia, sul tema "ITIL: MOTORE DEI SERVIZI", si terrà giovedì 8 maggio 2008, presso l'Hotel Villa Pamphili di via della Nocetta 105, a Roma. La vocazione nazionale di itSMF Italia ha trovato nelle dimensioni raggiunte nel 2007 le risorse indispensabili per le necessarie azioni concrete. La Conferenza di Primavera del 2007 - che ha raccolto a Roma oltre 300 manager e professionisti interessati ad ITIL - ha segnato il passaggio definitivo da una radicata presenza nel Nord-Ovest alla dimensione italiana.*

*Il pomeriggio sarà interamente dedicato alle testimonianze di progetti in fase avanzata di sviluppo. Ciascun relatore illustrerà il suo caso con una presentazione strutturata di circa 10 minuti. Per far emergere i punti di forza e le criticità nonché la specificità delle soluzioni singolarmente adottate, farà seguito un giro di tavola con domande rivolte alle aziende da un moderatore. E' inoltre previsto uno spazio per le domande del pubblico.*

*Il nostro auspicio è quello di raccogliere il meglio di quanto è stato realizzato finora in Italia, consentendoci di costruire la struttura della giornata in modo da renderla un momento gratificante per chi presenta e una esperienza importante di informazione e formazione per il pubblico professionale presente.*

*Disponibile sul sito dell'Associazione [l'agenda della giornata](#).*

*La partecipazione è gratuita previa [iscrizione online](#).*

*Considerato il successo di iscrizioni ai nostri passati Eventi che ci hanno costretti a spesso chiudere le adesioni in anticipo vi invitiamo quanti interessati ad iscriversi subito.*

*Cordiali saluti*

*Segreteria Operativa itSMF Italia  
[www.itsmf.it](http://www.itsmf.it)*

### **Il sito AIEA**

Continua la nostra lettura di chi, come e quando, accede al nostro sito. La distribuzione delle visite per ora, nel mese di aprile, è stata la seguente:



Ora	%	Ora	%
00 - 01	0,8%	12 - 13	10,3%
01 - 02	0,2%	13 - 14	5,3%
02 - 03	0,0%	14 - 15	8,0%
03 - 04	0,0%	15 - 16	8,2%
04 - 05	0,0%	16 - 17	7,1%
05 - 06	0,0%	17 - 18	8,4%
06 - 07	0,2%	18 - 19	5,9%
07 - 08	1,1%	19 - 20	2,8%
08 - 09	3,8%	20 - 21	1,8%
09 - 10	9,0%	21 - 22	2,5%
10 - 11	9,7%	22 - 23	2,0%
11 - 12	11,0%	23 - 24	1,7%

Mentre quelle per settimana, sempre nel mese di aprile, sono state:

Giorno	%
Lunedì	21,6%
Martedì	18,8%
Mercoledì	17,7%
Giovedì	18,2%
Venerdì	14,9%
Sabato	4,1%
Domenica	4,6%

Lunedì rimane il giorno con il maggior numero di accessi.

#### **Avviso ai soci**

Rinnoviamo l'invito ai soci di fornire le proprie indicazioni su argomenti o temi che desiderano vengano trattati nel corso del 2008 sia nelle Sessioni di studio sia in Workshop.

Chi volesse dare il proprio contributo, è pregato inviare una mail a [aiea@aiea.it](mailto:aiea@aiea.it), specificando, nell'oggetto "ARGOMENTI DI INTERESSE"

In una successiva newsletter provvederemo ad elencare tutti i temi proposti.

#### **Partecipazione di soci ad eventi**

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



---

Associazione Italiana  
Information Systems Auditors

---



In particolare, se partecipate ad un evento in qualità di organizzatore, relatore o chairman, 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!

#### Bibliografia

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

Vi informiamo che sul sito [www.cnipa.it](http://www.cnipa.it) sono disponibili molti documenti di interesse per i nostri soci. Ricordiamo che alla stesura di numerosi documenti hanno partecipato diversi nostri soci e che inoltre CNIPA organizza incontri o seminari aperti anche ai soci AIEA.



Associazione Italiana  
Information Systems Auditors



## ESTRATTO NEWSLETTER ANSSAIF DEL 7/4/2008

### Nuovo Consiglio Direttivo

L'Assemblea dei Soci, nell'approvare il bilancio dell'esercizio 2007 e le modifiche allo Statuto proposte dal Consiglio Direttivo, ha approvato all'unanimità la lista dei candidati al Consiglio Direttivo che resterà in carica per il biennio 2008-2009, così composto:

1. [Anthony Cecil WRIGHT](#) - Presidente
2. [Antonio CARICATO](#) - Segretario/Tesoriere
3. [Stefania PATAVIA](#)
4. [Giovanni BECATTINI](#)
5. [Vincenzo GIARDINA](#)
6. [Paolo GIUDICE](#)
7. [Stefano CABIANCA](#)
8. [Marco RECCHIA](#)
9. [Mario SESTITO](#)
10. [Massimiliano MAGI SPINETTI](#)
11. [Armando RIGHETTI](#)
12. [Leonardo PROCOPIO](#)
13. [Anna RYOLO](#)
14. [Alain DE CRISTOFARIS](#)
15. [Romain DEFLINE](#)
16. [Marco BEOZZI](#)

Un caloroso benvenuto alle "new entry" ed, in particolare a Anna RYOLO, Alain DE CRISTOFARIS, Romain DEFLINE e Marco BEOZZI

### Comitato Scientifico

Il Consiglio Direttivo, nella riunione del 26 gennaio c.a., ha deliberato all'unanimità di costituire il Comitato Scientifico delegando il Presidente ad avviare dei contatti con personalità che, riconosciute competenti nel settore di appartenenza e sensibili alle tematiche che ci occupano, possano essere di indirizzo all'Associazione.

Contatti più che proficui considerato che hanno accettato di far parte del Comitato Scientifico dell'ANSSAIF le seguenti personalità:

- Dott. Carlo Tresoldi, Presidente SIASSB SpA, già Direttore Centrale Banca d'Italia;
- Prof. [Michele Crudele](#), Direttore Didattico Centro ELIS e docente di Informatica;
- Dott. Luigi Di Marco, Past President Associazione Italiana per la Direzione del Personale;
- Prof. Alessandro Neri, professore ordinario di elettronica applicata presso la Facoltà di Ingegneria dell'Università di Roma Tre;
- Prof. Avv. Piero Sandulli, Ordinario di diritto processuale civile e di diritto processuale del lavoro;

Dott. Antonio Tarola, già Dirigente Banca d'Italia

Sicurezza in Internet: un sito su mille è pericoloso



Associazione Italiana  
Information Systems Auditors



Google ha studiato il grado di pericolosità dei siti Web, ossia la capacità che questi hanno di trasmettere al computer dell'utente malware o virus. Il risultato è che 1 sito su 1000 è infetto, ossia una totalità di oltre tre milioni di siti.

Nella ricerca di Google vengono anche elencati i paesi da cui più frequentemente provengono siti dannosi per i navigatori. Al primo posto ci sono i siti cinesi, da cui proviene il 67% dei casi di siti virulenti. A seguire, per quello che riguarda i siti di distribuzione dei malware, ci sono gli Stati Uniti, con il 15%, e la Russia, con il 4%. Nella top ten poi ci sono la Malesia con il 2,2%, la Corea con il 2%, Panama con l'1,1%, la Germania con l'1%, Hong Kong, la Turchia e la Francia con percentuali inferiori all'1%.

Un altro aspetto dello studio riguarda la frequenza con cui un utente che esegue una ricerca su un motore come Google si imbatte in un sito infetto: la quota è dell'1,3%.

[Per visionare/sc caricare lo studio completo.](#)

Garante della Privacy: piano ispettivo primo semestre 2008

Il Garante della Privacy, nella newsletter NUMERO 304 del 7 aprile 2008, ha anticipato quali saranno i principali settori dell'attività ispettiva programmata per il semestre in corso e, precisamente: sistemi di videosorveglianza, anagrafe tributaria, istituti di credito, banche dati di consulenti e periti.

Le verifiche dell'Autorità, effettuate anche in collaborazione con la Guardia di finanza, sul rispetto delle norme saranno indirizzate prioritariamente ai trattamenti di dati personali svolti dall'amministrazione finanziaria, mediante il sistema informativo della fiscalità, e dagli istituti di credito, per questi ultimi anche in riferimento al tracciamento degli accessi. Il programma prevede anche accertamenti sui trattamenti di dati svolti da parte di periti e consulenti.

Nell'ambito dell'attività ispettiva programmata, una particolare attenzione verrà posta ai sistemi di videosorveglianza. Saranno effettuate ispezioni su tutto il territorio nazionale sia per verificare il rispetto delle regole fissate dal Garante con il provvedimento del 2004 sull'uso delle telecamere, sia per poter disporre di un quadro aggiornato sull'attuale impiego dei sistemi di videosorveglianza da parte di soggetti pubblici e privati. Altri controlli in loco riguarderanno il rispetto dell'obbligo dell'informativa da fornire agli interessati al momento della raccolta dei dati personali, la libertà e validità del consenso, la durata della conservazione dei dati.

Saranno, inoltre, effettuate verifiche sull'adozione delle misure minime di sicurezza da parte di soggetti, pubblici e privati, che effettuano trattamenti di dati sensibili. Oltre agli accertamenti previsti nel programma varato, l'Ufficio svolgerà le ordinarie ulteriori attività istruttorie di carattere ispettivo relative a segnalazioni, reclami e ricorsi presentati all'Autorità.

Diffusione del malware

**F-Secure**, noto produttore di soluzioni per la sicurezza informatica, ha appena pubblicato un documento con il quale riassume il panorama delle minacce veicolate attraverso la rete Internet e, contemporaneamente, pubblica alcune previsioni sulle tendenze alle quali assisteremo nei prossimi mesi.

I laboratori di F-Secure giornalmente ricevono una media di 25.000 malware: con tali numeri, è facile



---

Associazione Italiana  
Information Systems Auditors

---



diagnosticare che il numero totale di virus e trojan, alla fine del 2008, supererà il traguardo del milione.

Poiché ogni azienda filtra oggi gli allegati dei messaggi di posta elettronica, questo approccio è divenuto meno efficace e, di conseguenza, le tecniche di diffusione hanno subito modifiche sostanziali. Gli attacchi vengono eseguiti utilizzando soluzioni "*drive-by download*": il codice nocivo viene ospitato sul web e gli utenti sono spronati a scaricarlo cliccando, ad esempio, su link inseriti in messaggi ricevuti via e-mail.

Questo genere di infezione si può verificare non appena un utente visita un sito web "maligno" utilizzando un sistema che non è stato opportunamente "messo in sicurezza" mediante la tempestiva applicazione della patch disponibili. L'aggressore, sfruttando le vulnerabilità non sanate, insite nel browser o nel sistema operativo dell'utente, può così riuscire ad installare automaticamente dei programmi dannosi sul semplicemente persuadendo l'utente a visitare una pagina web allestita allo scopo.

Sono molti gli espedienti utilizzati per indurre uno sprovveduto utente a visitare una pagina web "maligna": generalment, l'aggressore avvia delle campagne di spam inserendo, nel corpo del messaggio, testi simili ai seguenti: "*C'è un video che ti interessa su YouTube*", "*Hai ricevuto una cartolina d'auguri*" oppure, ancora, "*Grazie per il tuo ordine*", "*Ho acquistato l'oggetto che hai messo in vendita: comunicami le modalità di pagamento*". Cliccando sui link proposti, il browser viene condotto sulla pagina web dannosa.

Un altro metodo assai diffuso per la distribuzione di malware consiste nello sfruttare vulnerabilità di siti web famosi e comunemente ritenuti fidati per insediare codice dannoso.



Associazione Italiana  
Information Systems Auditors



## ESTRATTO NEWSLETTER ANSSAIF DEL 18/4/2008

### La sicurezza si studia sui banchi

Nell'ultima newsletter ([n. 05/2008](#))

che sono restie ad assumersi o, molto più spesso, che non sono in grado di svolgere.

Dove non arrivano le famiglie, arriva lo stato: la Virginia è il primo stato a rendere obbligatorie le lezioni di educazione alla sicurezza online, anche se i corsi si svolgono anche nelle scuole di Texas e Illinois. Sono inoltre numerosi i governi che stanno valutando l'introduzione di analoghi provvedimenti, spinti dalla crescente apprensione dei genitori nei confronti di dati e vicende a cui i media fanno da cassa di risonanza.

L'azione informativa in Virginia non si rivolge ai soli studenti come una costrizione, ma si coinvolgono le stesse famiglie per educarle ad una vigilanza responsabile dei propri figli mediante:

una descrizione dei filtri e di tecnologie di "parental control"  
invitando i genitori a non abbandonare i ragazzi davanti allo schermo,  
invitando i genitori a stabilire con i ragazzi un dialogo che li educi a schivare i pericoli che gli si parano di fronte, dentro e fuori dallo schermo.

Una guida proposta da "Virginia Department of Education" dal titolo "*INTERNET SAFETY IN SCHOOL*" è disponibile [QUI](#).

### Convegno 28 maggio 2008 in SIA SSB

Come già anticipato, nella giornata di Mercoledì 28 maggio 2008, ospitato dalla SIASSB SpA, si terrà a Milano, in Via Taramelli n. 26, il Convegno organizzato da ANSSAIF dal titolo

### LA SICUREZZA PER PREVENIRE, LA GESTIONE DELL'EMERGENZA PER RISPONDERE

Il convegno vuole costituire un momento di confronto ed interscambio delle conoscenze nella gestione di una crisi e si pone come obiettivo quello di:





Associazione Italiana  
Information Systems Auditors



Gli apparecchi colpiti sono solitamente quelli dotati di sistema operativo Symbian e, oltre a blindarne i dati contenuti, tenta di carpire informazioni tecniche (come la versione del sistema utilizzato sullo smartphone) e capaci di identificare l'apparecchio (come il codice IMEI).

Il suggerimento è sempre lo stesso, da applicarsi con adeguati accorgimenti tanto nel mondo dei computer quanto su quello degli smartphone: **non acconsentire mai l'installazione di un'applicazione sconosciuta dopo il download di un file**, soprattutto se proveniente da una fonte non conosciuta.

### **Collegio dei Proviviri**

Nell'ultimo Consiglio Direttivo del 26.01.2008 era stato dato mandato al Presidente di individuare figure di adeguato rango e professionalità per dare attuazione a quanto previsto all'art. 24 dello Statuto, ovvero la costituzione del *Collegio dei Proviviri*

Le personalità contattate dal Presidente hanno manifestato la loro disponibilità ed accettato la carica per il triennio 2008-2010.

Poichè di recente i Soci hanno a maggioranza approvato i nomi proposti, si comunica che, per il biennio 2008-2010, il Collegio dei Proviviri - ai quali i soci e gli aspiranti soci potranno rivolgersi per l'esame dei provvedimenti del Consiglio Direttivo che li riguardano - è costituito dai seguenti Signori:

1. **Paolo GIUDICE**: socio fondatore ANSSAIF, attuale Consigliere in carica e Segretario Generale CLUSIT
2. **Elio CIACCIA**: Presidente SIMPRESA e Consigliere CNEL
3. **Silvano ONGETTA**: Presidente AIEA

Il Collegio può essere contattato per email al seguente indirizzo: [proviviri@anssaif.eu](mailto:proviviri@anssaif.eu).

### **Superficialità e ignoranza = INSICUREZZA**

Un recente sondaggio (primi mesi del 2008) della NCSA (*National Cyber Security Alliance*) tra utenti di internet di età compresa tra 18 e 65 anni, ha fatto emergere una allarmante ignoranza sulle tematiche legate al crimine informatico.

Le risultanze più significative del sondaggio:

- ? la maggior parte degli intervistati ha dichiarato di essere consapevole del fatto che il proprio computer possa essere attaccato;
- ? il 59% non ritiene possibile che il proprio computer possa essere utilizzato come "ponte" per sferrare attacchi contro altri sistemi collegati alla rete;
- ? il 47% non ritiene possibile che il proprio computer possa essere controllato a distanza da qualcuno;
- ? il 51% non cambia la propria password da oltre un anno;



Associazione Italiana  
Information Systems Auditors



? il 48% non ha le idee chiare su come proteggersi dai cybercriminali.

I risultati di tale sondaggio, tuttavia, non fanno altro che confermare i risultati di uno studio concluso nell'ultimo trimestre del 2007 e condotto sempre dalla NCSA insieme a **McAfee**, Socio Sostenitore dell'ANSSAIF

I risultati più significativi di tale studio:

- ? solo il 55% degli intervistati aveva dichiarato di fare uso di programmi antispyware
- ? il 94% aveva dichiarato di avere installato un antivirus, ma il 48% utilizzava una versione scaduta;
- ? il 65% tra quelli che avevano un antivirus installato, non scaricava periodicamente gli aggiornamenti;
- ? l'81% degli intervistati dichiarava di avere un firewall installato, ma solo il 64% lo manteneva attivo;
- ? il 98% fra coloro che si proteggevano con programmi appositi riconoscevano l'importanza degli aggiornamenti, ma in realtà il 48% non effettuava un update del proprio sistema da almeno un mese.

I dati divulgati rendono ancora più evidente il fatto che non applicando misure di protezione al proprio computer, si agevolano in concreto le organizzazioni criminali (in quanto di questo oggi si tratta) che operano sulla rete a portare a compimento le attività fraudolente.

E, dato ancora più significativo, non fanno che evidenziare ancora di più la **necessità di educare aziende ed utenti sul tema della sicurezza informatica.**

Cultura della sicurezza informatica che tende a divenire, di fatto, una prima barriera a quello che sta diventando uno dei rischi più diffusi e più paventati dagli utenti, ossia

il **FURTO DELLA PRIVACY** o **FURTO D'IDENTITÀ**.



Associazione Italiana  
Information Systems Auditors



**ESTRATTO Newsletter CLUSIT del 30 aprile 2008- [www.clusit.it](http://www.clusit.it)**

**[disponibile in PDF all'indirizzo [www.clusit.net/newsletter\\_30\\_04\\_08.pdf](http://www.clusit.net/newsletter_30_04_08.pdf)]**

=====  
SANS AGGIORNA LE TOP 20 INTERNET SECURITY VULNERABILITIES  
=====

È disponibile in italiano l'ultimo aggiornamento di un documento del SANS Institute sulle 20 vulnerabilità più critiche per la sicurezza su internet. La versione italiana ([www.clusit.net/whitepapers/080408\\_top20\\_2007.pdf](http://www.clusit.net/whitepapers/080408_top20_2007.pdf)) è stata realizzata da Data Security, con il patrocinio del Clusit. Ringraziamo Romano Favero (Data Security) ed il SANS Institute, che ci hanno consentito la divulgazione del documento, e Luca Spingolo e Simone Brun, che hanno collaborato alla localizzazione italiana della SANS Top 20.

=====  
CYBERCRIME  
=====

Approvata la legge di ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica. Dopo l'approvazione il 20 febbraio 2008 da parte della Camera dei deputati, il Senato ha definitivamente approvato il disegno di legge A.S. n. 2012 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno". Il disegno legge è disponibile sul sito del Senato. [www.senato.it/japp/bgt/showdoc/showText?tipodoc=Ddlmess&leg=15&id=00298813&offset=445&length=26672&parse=no&stampa=si](http://www.senato.it/japp/bgt/showdoc/showText?tipodoc=Ddlmess&leg=15&id=00298813&offset=445&length=26672&parse=no&stampa=si)

-----  
Sicurezza in Internet: un sito su mille è pericoloso. Google ha studiato il grado di pericolosità dei siti Web, ossia la capacità che questi hanno di trasmettere al computer dell'utente malware o virus. Il risultato è che 1 sito su 1000 è infetto, ossia una totalità di oltre tre milioni di siti. Nella ricerca di Google vengono anche elencati i paesi da cui più frequentemente provengono siti dannosi per i navigatori. Al primo posto ci sono i siti cinesi, da cui proviene il 67% dei casi di siti virulenti. A seguire, per quello che riguarda i siti di distribuzione dei malware, ci sono gli Stati Uniti, con il 15%, e la Russia, con il 4%. Nella top ten poi ci sono la Malesia con il 2,2%, la Corea con il 2%, Panama con l'1,1%, la Germania con l'1%, Hong Kong, la Turchia e la Francia con percentuali inferiori all'1%. Un altro aspetto dello studio riguarda la frequenza con cui un utente che esegue una ricerca su un motore come Google si imbatte in un sito infetto: la quota è dell'1,3%. È possibile visionare/scaricare lo studio completo su <http://research.google.com/archive/provos-2008a.pdf>  
(Fonte: ANSSAIF - [www.anssaif.it](http://www.anssaif.it))

-----  
Nuovo Trojan per cellulari.



Si sta diffondendo in maniera massiccia un nuovo tipo di trojan che ha l'obiettivo di "sequestrare" i dati memorizzati su uno Smartphone o pDA-Phone e di rilasciarli solamente dietro il pagamento di un riscatto. Scaricando, anche via Bluetooth, un'applicazione apparentemente innocua, la stessa si annida nel dispositivo per infettarlo con una serie di virus e genera un SMS che compare sul display dello stesso apparecchio. Il proprietario dell'hardware si vede in sostanza apparire un messaggio (in lingua inglese) del tipo (tradotto) "Attenzione, il tuo apparecchio è infetto. Per favore, prepara 50 yuan e poi contatta il numero QQ nnnnnnnn". In pratica si richiede l'equivalente di circa sette euro per il "rilascio" dei dati presi in ostaggio, da versare mediante un sistema di pagamento online. Gli apparecchi colpiti sono solitamente quelli dotati di sistema operativo Symbian e, oltre a blindarne i dati contenuti, tenta di carpire informazioni tecniche (come la versione del sistema utilizzato sullo smartphone) e capaci di identificare l'apparecchio (come il codice IMEI). Il suggerimento è sempre lo stesso, da applicarsi con adeguati accorgimenti tanto nel mondo dei computer quanto su quello degli smartphone: non acconsentire mai l'installazione di un'applicazione sconosciuta dopo il download di un file, soprattutto se proveniente da una fonte non conosciuta.

(Fonte: ANSSAIF - [www.anssaif.it](http://www.anssaif.it))

=====  
DIFENDERSI DAGLI SPAM-BOT  
=====

Come si poteva facilmente prevedere, la battaglia con gli spammer sta dimostrando una nuova escalation. I punti d'attacco preferiti dagli spammer sono ovviamente gli account gratuiti di servizi quali Hotmail, Yahoo, Gmail, o anche i nostri Libero, Katamail, e così via. Poter spedire da uno di questi account significa poter aggirare numerose blacklist, ed anche parecchi filtri basati sulla reputazione del mittente, perché ovviamente non è possibile rifiutare posta integralmente da questi domini, e farlo per singola casella è comunque oneroso. Praticamente tutti questi fornitori richiedono, durante la registrazione, di riconoscere ed inserire una stringa alfanumerica più o meno "oscurata" distorcendone i caratteri, modificandone lo sfondo, sovrapponendo righe ed altri disturbi, sistema che viene definito con la sigla CAPTCHA. Teoricamente, per un essere umano è comunque facile venirne a capo, e per una macchina è difficilissimo. Teoricamente: perché, con il continuo miglioramento dei software OCR, per le macchine diventa sempre più facile. I CAPTCHA diventano quindi sempre più oscurati, al punto che oggi non è facile nemmeno per una persona riconoscere la scritta. Come peraltro riporta un articolo di Network World [www.networkworld.com/news/2008/041108-bot-breaks-hotmails-captcha-in.html?nethht=rn\\_041508&amp;](http://www.networkworld.com/news/2008/041108-bot-breaks-hotmails-captcha-in.html?nethht=rn_041508&amp;)

è stato rilevato un bot che si installa, come spesso accade, su un PC di un ignaro utente vulnerabile, e da lì tenta subito di registrare nuovi account su Hotmail per poi usarli per inviare spam. A quanto pare impiega circa sei secondi per riconoscere il CAPTCHA di Hotmail, ed anche se in realtà lo fa correttamente solo una volta su dieci, il punto è che ottiene comunque in breve tempo una grande quantità di account (in apparenza legittimi) da usare per inviare spam e potenzialmente replicarsi. Finora i CAPTCHA sono stati un po' il chinino dei freemail via Web, ma sembra che la loro malaria ormai sia diventata resistente. Occorre urgentemente trovare una molecola più efficace.

(Autore: Mauro Cicognini)

=====  
NOTIZIE DALL'EUROPA  
=====

Nuovo programma della Commissione europea per la sicurezza dei minori su internet.



Associazione Italiana  
Information Systems Auditors



Recentemente la Commissione europea ha proposto un nuovo programma per una maggiore sicurezza dei minori che navigano in linea. Di fronte alla diffusione recente di servizi di comunicazione del web 2.0, come i siti di socializzazione, il nuovo programma intende lottare non solo contro i contenuti illeciti, ma anche contro comportamenti dannosi come il bullismo in linea e l'adescamento in rete a scopi sessuali. Basandosi sul successo del precedente programma del 2005, il nuovo programma fruisce di una dotazione di bilancio di 55 milioni di euro e abbraccia il periodo 2009-2013.

Maggiori dettagli nel comunicato stampa della Commissione europea.

<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/310&format=PDF&aged=0&language=IT&guiLanguage=fr>

Nuovo portale dell'Unione Europea sulla sicurezza. Il portale della DG Information Society dedicato alla sicurezza delle informazioni è stato ridisegnato e modificato.

([http://ec.europa.eu/information\\_society/policy/nis/index\\_en.htm](http://ec.europa.eu/information_society/policy/nis/index_en.htm)).

Da segnalare la disponibilità delle relazioni del seminario di fine 2007 sul tema della security awareness

([http://ec.europa.eu/information\\_society/policy/nis/strategy/activities/awareness\\_seminar/index\\_en.htm](http://ec.europa.eu/information_society/policy/nis/strategy/activities/awareness_seminar/index_en.htm)),

particolarmente utile e interessante, soprattutto la presentazione del prof Rigidel del ENST di Parigi

([http://ec.europa.eu/information\\_society/policy/nis/docs/wshop/keynote\\_speech\\_rigidel.pdf](http://ec.europa.eu/information_society/policy/nis/docs/wshop/keynote_speech_rigidel.pdf)).

Report - attacchi su larga scala. La DG Internet Society ha pubblicato il report dell'incontro di gennaio che ha analizzato le implicazioni che derivano dagli attacchi su larga scala. Il report è disponibile su

[http://ec.europa.eu/information\\_society/policy/nis/docs/largescaleattacksdocs/Report\\_Internet\\_Security\\_WS\\_170108.pdf](http://ec.europa.eu/information_society/policy/nis/docs/largescaleattacksdocs/Report_Internet_Security_WS_170108.pdf)

Le relazioni e le slide su

[http://ec.europa.eu/information\\_society/policy/nis/strategy/activities/ciip/large\\_scale/index\\_en.htm](http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/index_en.htm)

> Interessanti calls for proposal.  
> C'è "fermento" alla UE in tema di sicurezza e sicuramente ci possono essere opportunità per i soci CLUSIT, cui raccomandiamo di leggere con attenzione i "Call for proposal" che potrebbero essere interessanti per le imprese o anche per i singoli.  
> Qui di seguito ne segnaliamo uno con scadenza a breve che vale la pena di leggere.  
> <http://blog.clusit.it/sicuramente/2008/04/attenzione-ai-c.html#more>

> Gruppo di lavoro di ENISA sulle microimprese.  
> Qualche giorno fa ho partecipato a nome del CLUSIT alla prima riunione del gruppo di lavoro di ENISA (European Network and Information Security Agency) sulle microimprese. I problemi di sicurezza delle piccole imprese e delle microimprese sono gli stessi in tutta Europa, e quindi la collaborazione a questo livello può aiutare ad affrontare un settore che, dati i numeri in gioco (milioni di piccole imprese e microimprese) richiede una strategia e strumenti specifici. Per ora posso dire che lo scambio di informazioni e di esperienze all'interno del gruppo è



> estremamente interessante, e aiuterà il CLUSIT nelle sue iniziative in  
> questo settore. Prossimamente vi darò maggiori informazioni sia  
> sull'attività del gruppo di lavoro di ENISA che sulle iniziative del  
> CLUSIT per le PMI.  
> (Autore: Claudio Telmon, coordinatore del progetto Clusit "Rischio IT e  
> piccola impresa")

=====  
NOTIZIE DAGLI USA

=====  
La sicurezza si studia sui banchi di scuola. Si segnala che negli Stati Uniti, nello stato della Virginia, la sicurezza sul Web è divenuta una nuova materia di insegnamento: i ragazzi vengono istruiti riguardo ai pericoli che corrono in rete e vengono addestrati all'autodifesa sul Web. A disporre che la materia entri a far parte del piano formativo dei ragazzi fra gli 11 e i 16 anni, è stato il Ministero dell'Istruzione locale: i corsi sono attivi, alcuni ragazzi sono attenti, alcune famiglie sono felici di delegare alle agenzie educative un compito che sono restie ad assumersi o, molto più spesso, che non sono in grado di svolgere.....  
Una guida proposta da "Virginia Department of Education", dal titolo "INTERNET SAFETY IN SCHOOL", è disponibile su [www.anssaif.it/allegati/internet-safety-guidelines-resources.pdf](http://www.anssaif.it/allegati/internet-safety-guidelines-resources.pdf) (Fonte: ANSSAIF - [www.anssaif.it](http://www.anssaif.it))

=====  
EVENTI SICUREZZA

=====  
22 maggio 2008, Roma\*  
Seminario Clusit - Computer forensics: aspetti legali e strumenti operativi

4 giugno 2008, Bologna\*\*  
Seminario Clusit: Dal Penetration Testing alla Risk Analysis: la metodologia OSSTMM 3.0, lo standard ISO 27001 ed i punti di incontro

5 giugno 2008, Firenze\*\*  
Seminario Clusit: Dal Penetration Testing alla Risk Analysis: la metodologia OSSTMM 3.0, lo standard ISO 27001 ed i punti di incontro

10-11 giugno 2008, Roma  
Infosecurity Italia - Storage Expo - trackability  
[www.infosecurity.it/IT/roadshow/roma%202008.aspx](http://www.infosecurity.it/IT/roadshow/roma%202008.aspx)

10 giugno 2008, Roma\*\*  
Seminario Clusit: Dal Penetration Testing alla Risk Analysis: la metodologia OSSTMM 3.0, lo standard ISO 27001 ed i punti di incontro

\* Posti esauriti

\*\*La registrazione ai seminari, temporaneamente sospesa per motivi tecnici, sarà disponibile entro alcuni giorni su <https://edu.clusit.it>

=====

Legge 18 marzo 2008, n. 48

**"Ratifica ed esecuzione della Convenzione del Consiglio d' Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell' ordinamento interno"**

pubblicata nella *Gazzetta Ufficiale* n. 80 del 4 aprile 2008 - Supplemento ordinario n. 79

---

Capo I

RATIFICA ED ESECUZIONE

Art. 1.

*(Autorizzazione alla ratifica)*

1. Il Presidente della Repubblica è autorizzato a ratificare la Convenzione del Consiglio d' Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, di seguito denominata «Convenzione».

Art. 2.

*(Ordine di esecuzione)*

1. Piena e intera esecuzione è data alla Convenzione, a decorrere dalla data della sua entrata in vigore in conformità a quanto disposto dall' articolo 36 della Convenzione stessa.

Capo II

MODIFICHE AL CODICE PENALE E AL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231

Art. 3.

*(Modifiche al titolo VII del libro secondo del codice penale)*

1. All' articolo 491<sup>bis</sup> del codice penale sono apportate le seguenti modificazioni:

*a)* al primo periodo, dopo la parola: «privato» sono inserite le seguenti: «avente efficacia probatoria»;

*b)* il secondo periodo è soppresso.

2. Dopo l' articolo 495 del codice penale è inserito il seguente:

«Art. 495-bis. – (*Falsa dichiarazione o attestazione al certificatore di firma elettronica sull' identità o su qualità personali proprie o altrui*). – Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l' identità o lo stato o altre qualità della propria o dell' altrui persona è punito con la reclusione fino ad un anno».

Art. 4.

(*Modifica al titolo XII del libro secondo del codice penale*)

1. L' articolo 615quinquies del codice penale è sostituito dal seguente:

«Art. 615-quinquies. – (*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*). – Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l' interruzione, totale o parziale, o l' alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329».

Art. 5.

(*Modifiche al titolo XIII del libro secondo del codice penale*)

1. L' articolo 635bis del codice penale è sostituito dal seguente:

«Art. 635-bis. – (*Danneggiamento di informazioni, dati e programmi informatici*). – Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell' articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d' ufficio».

2. Dopo l' articolo 635bis del codice penale sono inseriti i seguenti:

«Art. 635-ter. – (*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*). – Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l' alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell' articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Art. 635-quater. – (*Danneggiamento di sistemi informatici o telematici*). – Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all' articolo 635bis, ovvero attraverso l' introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia,

rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell' articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

*Art. 635-quinquies. – (Danneggiamento di sistemi informatici o telematici di pubblica utilità) .–* Se il fatto di cui all' articolo 635-*quater* è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell' articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata».

3. Dopo l' articolo 640-*quater* del codice penale è inserito il seguente:

«Art. 640-*quinquies*. – (*Frode informatica del soggetto che presta servizi di certificazione di firma elettronica*). – Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro».

Art. 6.

(*Modifiche all' articolo 420 del codice penale*)

1. All' articolo 420 del codice penale, il secondo e il terzo comma sono abrogati.

Art. 7.

(*Introduzione dell' articolo 24-bis del decreto legislativo 8 giugno 2001, n. 231*)

1. Dopo l' articolo 24 del decreto legislativo 8 giugno 2001, n. 231, è inserito il seguente:

«Art. 24-*bis*. – (*Delitti informatici e trattamento illecito di dati*). – 1. In relazione alla commissione dei delitti di cui agli articoli 615-*ter*, 617-*quater*, 617-*quinquies*, 635-*bis*, 635-*ter*, 635-*quater* e 635-*quinquies* del codice penale, si applica all' ente la sanzione pecuniaria da cento a cinquecento quote.

2. In relazione alla commissione dei delitti di cui agli articoli 615-*quater* e 615-*quinquies* del codice penale, si applica all' ente la sanzione pecuniaria sino a trecento quote.

3. In relazione alla commissione dei delitti di cui agli articoli 491-*bis* e 640-*quinquies* del codice penale, salvo quanto previsto dall' articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all' ente la sanzione pecuniaria sino a quattrocento quote.

4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall' articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall' articolo 9, comma 2,

lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall' articolo 9, comma 2, lettere c), d) ed e)».

### Capo III

## MODIFICHE AL CODICE DI PROCEDURA PENALE E AL CODICE DI CUI AL DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196

### Art. 8.

*(Modifiche al titolo III del libro terzo del codice di procedura penale)*

1. All' articolo 244, comma 2, secondo periodo del codice di procedura penale sono aggiunte, in fine, le seguenti parole: «, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l' alterazione».

2. All' articolo 247 del codice di procedura penale, dopo il comma 1 è inserito il seguente:

«I-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l' alterazione».

3. All' articolo 248, comma 2, primo periodo, del codice di procedura penale, le parole: «atti, documenti e corrispondenza presso banche» sono sostituite dalle seguenti: «presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici».

4. All' articolo 254 del codice di procedura penale sono apportate le seguenti modificazioni:

a) il comma 1 è sostituito dal seguente:

«1. Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l' autorità giudiziaria abbia fondato motivo di ritenere spediti dall' imputato o a lui diretti anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato»;

b) al comma 2, dopo le parole: «senza aprirli» sono inserite le seguenti: «o alterarli».

5. Dopo l' articolo 254 del codice di procedura penale è inserito il seguente:

«Art. 254-bis. – (Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni). – 1. L' autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali».

6. All' articolo 256, comma 1, del codice di procedura penale, dopo le parole: «anche in originale se così è ordinato,» sono inserite le seguenti: «nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto,».

7. All' articolo 259, comma 2, del codice di procedura penale, dopo il primo periodo è inserito il seguente: «Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell' obbligo di impedirne l' alterazione o l' accesso da parte di terzi, salva, in quest' ultimo caso, diversa disposizione dell' autorità giudiziaria».

8. All' articolo 260 del codice di procedura penale sono apportate le seguenti modificazioni:

a) al comma 1, dopo le parole: «con altro mezzo» sono inserite le seguenti: «, anche di carattere elettronico o informatico,»;

b) al comma 2 è aggiunto, in fine, il seguente periodo: «Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all' originale e la sua immodificabilità ; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria».

#### Art. 9.

*(Modifiche al titolo IV del libro quinto del codice di procedura penale)*

1. All' articolo 352 del codice di procedura penale, dopo il comma 1 è inserito il seguente:

«I-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l' alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi».

2. All' articolo 353 del codice di procedura penale sono apportate le seguenti modificazioni:

a) al comma 2 sono aggiunte, in fine, le seguenti parole: «e l' accertamento del contenuto»;

b) al comma 3, primo periodo, le parole: «lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza» sono sostituite dalle seguenti: «lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza, anche se in forma elettronica o se inoltrati per via telematica,» e dopo le parole: «servizio postale» sono inserite le seguenti: «, telegrafico, telematico o di telecomunicazione».

3. All' articolo 354, comma 2, del codice di procedura penale, dopo il primo periodo è inserito il seguente: «In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l' alterazione e l' accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all' originale e la sua immodificabilità ».

#### Art. 10.

*(Modifiche all' articolo 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196)*

1. Dopo il comma 4-bis dell' articolo 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, sono inseriti i seguenti:

«4-ter. Il Ministro dell' interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell' Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell' articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l' eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.

4-quater. Il fornitore o l' operatore di servizi informatici o telematici cui è rivolto l' ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all' autorità richiedente l' assicurazione dell' adempimento. Il fornitore o operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all' ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall' autorità. In caso di violazione dell' obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell' articolo 326 del codice penale.

4-quinqies. I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia».

#### Art. 11.

##### *(Competenza)*

1. All' articolo 51 del codice di procedura penale è aggiunto, in fine, il seguente comma:

«3-quinqies. Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 600-bis, 600-ter, 600-quater, 600-quater.1, 600-quinqies, 615-ter, 615-quater, 615-quinqies, 617-bis, 617-ter, 617-quater, 617-quinqies, 617-sexies, 635-bis, 635-ter, 635-quater, 640-ter e 640-quinqies del codice penale, le funzioni indicate nel comma 1, lettera a), del presente articolo sono attribuite all' ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente».

#### Art. 12.

##### *(Fondo per il contrasto della pedopornografia su internet e per la protezione delle infrastrutture informatiche di interesse nazionale)*

1. Per le esigenze connesse al funzionamento del Centro nazionale per il contrasto della pedopornografia sulla rete INTERNET, di cui all' articolo 14-bis della legge 3 agosto 1998, n. 269, e dell' organo del Ministero dell' interno per la sicurezza e per la regolarità dei servizi di telecomunicazione per le esigenze relative alla protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale, di cui all' articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, è istituito, nello stato di

previsione del Ministero dell' interno, un fondo con una dotazione di 2 milioni di euro annui a decorrere dall' anno 2008.

2. Agli oneri derivanti dal presente articolo, pari a 2 milioni di euro annui a decorrere dall' anno 2008, si provvede mediante corrispondente riduzione dello stanziamento iscritto, ai fini del bilancio triennale 2008-2010, nell' ambito del fondo speciale di parte corrente dello stato di previsione del Ministero dell' economia e delle finanze per l' anno 2008, allo scopo parzialmente utilizzando l' accantonamento relativo al Ministero della giustizia.

3. Il Ministro dell' economia e delle finanze è autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.

#### Capo IV

#### DISPOSIZIONI FINALI

##### Art. 13.

*(Norma di adeguamento)*

1. L' autorità centrale ai sensi degli articoli 24, paragrafo 7, e 27, paragrafo 2, della Convenzione è il Ministro della giustizia.

2. Il Ministro dell' interno, di concerto con il Ministro della giustizia, individua il punto di contatto di cui all' articolo 35 della Convenzione.

##### Art. 14.

*(Entrata in vigore)*

1. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella *Gazzetta Ufficiale*.

## *Reati informatici ex art. 24 bis Decreto 231/01*

La Legge 48/08 di ratifica della Convenzione sulla Criminalità Informatica - pubblicata sulla Gazzetta Ufficiale della Repubblica Italiana n. 80 del 4 aprile u.s., Supplemento Ordinario n. 79 (di seguito allegata) - ha esteso, a far data dal 5 aprile u.s., la responsabilità amministrativa delle persone giuridiche ai reati di "criminalità informatica".

In particolare, la citata Legge ha introdotto nel D.Lgs. 231/01 l'art. 24-bis, che fa riferimento ai seguenti reati:

- falsità in un documento informatico pubblico o privato (491-bis c.p.)
- accesso abusivo ad un sistema informatico o telematico (615-ter c.p.)
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (615-quater c.p.)
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (615-quinquies c.p.)
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (617-quater c.p.)
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (617-quinquies c.p.)
- danneggiamento di informazioni, dati e programmi informatici (635-bis c.p.)
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (635-ter c. p.)
- danneggiamento di sistemi informatici o telematici (635-quater c.p.)
- danneggiamento di sistemi informatici o telematici di pubblica utilità (635-quinquies c.p.)
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (640-quinquies c.p.)

I reati citati si riferiscono, in via meramente esemplificativa e non esaustiva, alle seguenti possibili condotte, realizzate sempre nell'interesse o a vantaggio dell'ente:

- alterazione di documenti elettronici, pubblici o privati, con finalità probatoria
- creazioni/modifiche/cancellazioni fraudolente di dati di enti concorrenti, pubblici o privati
- accesso abusivo all'intranet di enti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate commerciali o industriali
- modifiche non autorizzate a programmi al fine di danneggiare enti concorrenti, pubblici o privati

- detenzione ed utilizzo abusivo di password di accesso a siti di enti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate commerciali o industriali
- intercettazione fraudolenta di comunicazioni di enti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate commerciali o industriali
- installazione fraudolenta di dispositivi per intercettazioni telefoniche e radio di enti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate commerciali o industriali
- diffusione tramite la rete aziendale di programmi illeciti o virus con la finalità di danneggiare enti concorrenti, pubblici o privati
- danneggiamento di strumenti di commercio elettronico di enti concorrenti, pubblici o privati
- modifica fraudolenta di informazioni di enti concorrenti, pubblici o privati

A fronte di questi delitti, l'ente è punito con sanzioni pecuniarie da cento a cinquecento quote nonché con le sanzioni interdittive di cui all'art. 9 del D.Lgs. 231/01, a seconda della fattispecie di reato.

Tale emendamento amplia la responsabilità amministrativa degli enti rendendo necessaria la verifica e l'eventuale aggiornamento dei Modelli organizzativi ex D.Lgs. 231/01 anche ai fini di valutare la rispondenza dei sistemi informativi - che rappresentano una componente rilevante dei sistemi di gestione e controllo aziendali - ai requisiti di legge e l'adeguatezza dei relativi presidi di controllo rispetto alle esigenze di tutela della società.

In considerazione del fatto che i nuovi ambiti applicativi della norma richiedono specifiche competenze tecniche per l'analisi delle possibili modalità di realizzazione, per la valutazione dei rischi informatici associati nonché per la verifica e successiva definizione dei relativi presidi di controllo, Protiviti è in grado di integrare le competenze ad oggi maturate sui temi "231" con un Team di consulenti esperti in servizi di Technology Risk Consulting, che potranno assistere - anche su questi temi - la Vostra organizzazione nell'aggiornamento dei Modelli "231" adottati.

Per maggiori informazioni, rivolgetevi all'ufficio Protiviti più vicino o contattate Luca Medizza, Massimo Minerva o Francesca Delfini al numero 02 6550 6301.



- CANONE RAI: CORRETTEZZA NEI SOLLECITI AGLI UTENTI
- IL PIANO ISPETTIVO DEL GARANTE PER IL PRIMO SEMESTRE 2008
- IN ARRIVO IL REGOLAMENTO SU DATI SENSIBILI E GIUDICARIZI DELLA SSPAL

## Canone Rai: correttezza nei solleciti agli utenti

Niente pressioni sugli utenti e informazioni più corrette da parte dei cosiddetti "ispettori Rai" incaricati di contattare le persone che non risultano abbonate per sollecitare la sottoscrizione del canone televisivo. Gli incaricati Rai che svolgono questo servizio per conto della Agenzia delle entrate devono tenere un comportamento trasparente e fornire agli utenti informazioni chiare sulla propria attività in modo da non ingenerare errori o equivoci sul loro effettivo ruolo. Al termine di un'istruttoria avviata nei mesi scorsi il Garante privacy (con un provvedimento di cui è stato relatore Giuseppe Chiaravalloti) ha prescritto all'Agenzia delle entrate - Sportello abbonamenti tv alcune misure per conformare alla normativa i trattamenti di dati effettuati dagli agenti incaricati sulla base della convenzione tra l'Agenzia e la Rai del 2001. Sono ancora numerose le segnalazioni che giungono all'Autorità in cui si lamentano comportamenti ritenuti irrispettosi di agenti Rai che, qualificandosi come "ispettori", si presenterebbero presso le abitazioni e con toni minacciosi e con modalità considerate "inquisitorie" o "intimidatorie" procederebbero alla ricerca degli evasori del canone televisivo e a sollecitare gli abbonamenti. Segnalati anche casi in cui, di fronte alla titubanza dei cittadini nel fornire determinate informazioni, sono stati minacciati accertamenti nelle abitazioni. Entro il 30 aprile l'Agenzia delle entrate dovrà comunicare al Garante le misure necessarie impartite ai suoi agenti affinché i trattamenti dei dati siano conformi al Codice privacy. L'Agenzia dovrà innanzitutto garantire che gli agenti Rai spieghino chiaramente agli utenti, senza artifici e senza indurli in errore, la loro esclusiva attività di promozione dell'abbonamento televisivo. L'Agenzia dovrà garantire, inoltre, che l'informativa sul trattamento dei dati indichi con precisione quali informazioni sia obbligatorio fornire e quali no. Da evitare, infine, pressioni indebite sugli utenti "minacciando" controlli intrusivi nelle abitazioni.

Con un autonomo procedimento l'Autorità ha aperto un'istruttoria per verificare la corretta applicazione delle

misure di sicurezza a protezione dei dati personali usati per il recupero dell'evasione del canone televisivo.

## Il piano ispettivo del Garante per il primo semestre 2008

Telecamere, anagrafe tributaria, banche, consulenti e periti sotto la lente dell'Autorità

Sistemi di videosorveglianza, anagrafe tributaria, istituti di credito, banche dati di consulenti e periti. Sono questi i principali settori dell'attività ispettiva programmata per il semestre in corso dal Garante per la protezione dei dati personali.

Le verifiche dell'Autorità, effettuate anche in collaborazione con la Guardia di finanza, sul rispetto delle norme saranno indirizzate prioritariamente ai trattamenti di dati personali svolti dall'amministrazione finanziaria, mediante il sistema informativo della fiscalità, e dagli istituti di credito, per questi ultimi anche in riferimento al tracciamento degli accessi. Il programma prevede anche accertamenti sui trattamenti di dati svolti da parte di periti e consulenti.

Nell'ambito dell'attività ispettiva programmata, una particolare attenzione verrà posta ai sistemi di videosorveglianza. Saranno effettuate ispezioni su tutto il territorio nazionale sia per verificare il rispetto delle regole fissate dal Garante con il provvedimento del 2004 sull'uso delle telecamere, sia per poter disporre di un quadro aggiornato sull'attuale impiego dei sistemi di videosorveglianza da parte di soggetti pubblici e privati. Altri controlli in loco riguarderanno il rispetto dell'obbligo dell'informativa da fornire agli interessati al momento della raccolta dei dati personali, la libertà e validità del consenso, la durata della conservazione dei dati.

Saranno, inoltre, effettuate verifiche sull'adozione delle misure minime di sicurezza da parte di soggetti, pubblici e privati, che effettuano trattamenti di dati sensibili.

Oltre agli accertamenti previsti nel programma varato, l'Ufficio svolgerà le ordinarie ulteriori attività istruttorie di carattere ispettivo relative a segnalazioni, reclami e ricorsi presentati all'Autorità.

# In arrivo il regolamento su dati sensibili e giudiziari della Sspal

Il Garante ribadisce la necessità di delimitare la consultazione diretta di banche dati e le interconnessioni tra sistemi informativi

Il Garante per la protezione dei dati personali ha espresso parere favorevole (relatore Giuseppe Fortunato) sullo schema di regolamento per il trattamento di dati sensibili e giudiziari predisposto dalla Scuola superiore della pubblica amministrazione locale a condizione che vengano apportate alcune modifiche e integrazioni.

L'Autorità ha innanzitutto invitato la Scuola superiore ad adottare un atto che, a differenza di quello predisposto, abbia un'effettiva natura regolamentare, in grado pertanto di produrre effetti giuridici per gli interessati.

Per quanto riguarda le operazioni eseguibili con i dati raccolti, il Garante ha chiesto di verificare se le operazioni di interconnessione e di raffronto con altre banche dati della Scuola e con l'Agenzia autonoma per la gestione dell'Albo dei segretari comunali e provinciali siano davvero indispensabili. Va delimitata, infatti, la consultazione diretta di banche dati e le interconnessioni tra sistemi informativi perché queste operazioni potrebbero determinare un'ingiustificata circolazione dei dati degli interessati. A tale proposito, l'Autorità ha disposto che i dati vengano trasmessi mediante un diverso tipo di collegamento informatico o telematico che consenta agli altri uffici della Scuola e ad altri soggetti pubblici di consultare i dati solo su richiesta.

Per quanto riguarda le tipologie di dati trattati, poi, il Garante ha precisato che il regolamento deve avere per oggetto esclusivamente informazioni sensibili e giudiziarie invitando a verificarne l'indispensabilità, in particolare per quanto riguarda l'uso di dati personali relativi allo stato di salute per le attività di studio e ricerca della Scuola che dovrebbero riguardare soltanto tematiche d'interesse per gli enti locali.

Ulteriori e successivi trattamenti di dati sensibili e giudiziari non considerati nello schema approvato dovranno essere sottoposti di nuovo al parere del Garante.

---

## 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](http://www.garanteprivacy.it)



- I NOMI DEGLI ALUNNI SUL SITO DEL CONSIGLIERE COMUNALE: INTERVIENE IL GARANTE
- 5 PER MILLE IRPEF: ELENCHI DEGLI AMMESSI SUL WEB, MA A NORMA DI LEGGE
- SÌ AI DATI BIOMETRICI DEI DIPENDENTI PER GARANTIRE LA SALUTE PUBBLICA

## I nomi degli alunni sul sito del consigliere comunale

Il Garante interviene su segnalazione dello stesso Comune

Un consigliere comunale mette sul suo sito web la lista nominativa degli alunni delle scuole medie inferiori, secondarie e superiori che hanno ottenuto il contributo per l'acquisto dei libri di testo. E il Garante privacy blocca l'uso dei dati.

Su segnalazione del Comune di Palau, l'Autorità ha bloccato (con un provvedimento di cui è stato relatore Mauro Paissan) il trattamento dei dati personali relativi alla lista con i nomi degli alunni delle scuole medie inferiori, secondarie e superiori che hanno ottenuto il contributo per l'acquisto dei libri di testo apparsa sul sito web del capogruppo consiliare di minoranza. Tante le informazioni personali pubblicate: i dati identificativi di alunni e genitori, l'ammontare del contributo economico erogato e in alcuni casi perfino le coordinate del conto corrente bancario.

Il Comune, che aveva segnalato all'Autorità la diffusione dei dati, aveva precisato di non averne dato pubblicità per evitare che i dati personali di natura economica divenissero facilmente di dominio pubblico. Gli elenchi, infatti, non erano stati affissi né all'albo pretorio, né erano stati pubblicati sul sito istituzionale perché secondo l'amministrazione comunale la loro diffusione poteva creare imbarazzo o disagio agli interessati, che appartengono a fasce deboli della popolazione, ed esporli a conseguenze indesiderate. Le informazioni erano comunque accessibili su richiesta. Una copia degli elenchi era stata consegnata anche al capogruppo di minoranza in ragione del suo mandato politico, il quale ha deciso invece di pubblicarla sul suo sito.

Il trattamento dei dati contenuti negli atti dell'amministrazione comunale - ha ricordato l'Autorità - può essere effettuato dai consiglieri in ragione del loro mandato, ma sempre nel rispetto del diritto alla riservatezza degli interessati. La pubblicazione su Internet di queste informazioni personali, rese in questo modo immediatamente accessibili a tutti attraverso una

semplice ricerca per nome, è risultata invece illecita, in particolare perché eccessiva rispetto alle finalità per le quali le informazioni erano state raccolte. Il Garante ha, pertanto, disposto in via d'urgenza il blocco dei dati diffusi dal sito in attesa di ulteriori accertamenti. Il consigliere, nel frattempo, dovrà limitarsi a conservare i dati senza poter compiere nessun'altra operazione di trattamento.

## 5 per mille Irpef: elenchi degli ammessi sul web, ma a norma di legge

E' possibile pubblicare gli elenchi dei soggetti ammessi, anche in via provvisoria, al beneficio del 5 per mille sul sito web dell'Agenzia delle entrate, ma occorre che ciò sia previsto da una norma di legge o di regolamento. È questo il parere "condizionato" espresso dal Garante (relatore Francesco Pizzetti) nell'esaminare lo schema di d.p.c.m. presentato dal Ministero della solidarietà sociale riguardante le modalità di richiesta di ammissione al beneficio del 5 per mille. Lo schema prevede che le associazioni di volontariato debbano trasmettere in via telematica all'Agenzia delle entrate - oppure, per gli enti della ricerca scientifica e dell'università, al Ministero dell'università e delle ricerca - una domanda di iscrizione in un apposito elenco.

Ad avviso del Garante, la messa a disposizione su Internet degli elenchi realizzerebbe una diffusione di dati personali: è, quindi, necessario che tale forma di pubblicazione sia specificamente prevista da una norma di legge o di regolamento che l'amministrazione dovrà individuare, come stabilito dal Codice privacy.

Oltre ad evidenziare l'esigenza di una specifica norma che consenta, dunque, tale diffusione, l'Autorità ha inoltre chiesto che i modelli di domanda per l'iscrizione telematica agli elenchi rechino un'informativa con le stesse caratteristiche di quella apposta in calce al modello cartaceo destinato all'Agenzia delle entrate e che sia opportunamente omessa l'informativa nel modello di autodichiarazione successivo, trattandosi

delle medesime informazioni e dello stesso procedimento.

## Sì ai dati biometrici dei dipendenti per garantire la salute pubblica

È possibile trattare dati biometrici dei dipendenti per specifiche e rilevanti finalità, come ad esempio la salute pubblica. È quanto ribadito dal Garante (con un provvedimento di cui è stato relatore Giuseppe Fortunato) nel ritenere lecito e conforme alla disciplina privacy il sistema di rilevazione biometrica proposto da una società di risorse idriche. La società chiedeva di poter utilizzare dati biometrici dei propri dipendenti al fine di monitorare gli accessi ad alcune aree dell'impresa, in particolare quelle in cui avviene la potabilizzazione dell'acqua, garantendo in questo modo la sicurezza dell'impianto idrico, la tutela della qualità delle acque e, di conseguenza, la salute pubblica. Il sistema di rilevazione biometrica sottoposto dalla società alla verifica preliminare del Garante prevede la registrazione delle impronte digitali dei dipendenti – rilasciate con il consenso degli stessi – attraverso apparecchiature e software appositi e la successiva trasformazione delle stesse impronte in codici numerici (*template*) inseriti in una smart card. In più si proponeva la memorizzazione dei dati relativi all'orario di accesso e dei codici che consentono di risalire all'identità del dipendente in una banca dati centralizzata. Nell'esaminare il progetto proposto dalla società, il Garante ha precisato che la raccolta delle impronte debba limitarsi ai soli dipendenti che hanno accesso all'area dell'impresa in cui avviene la depurazione delle acque e, soprattutto, che le impronte cifrate non debbano essere conservate in un archivio centralizzato ma solo su un supporto (una smart card ad esempio) nell'esclusiva disponibilità dell'interessato. Il Garante ha ricordato, infine, riprendendo quanto stabilito nelle Linee Guida in materia di trattamento dei dati personali dei lavoratori, che tutti i dati raccolti relativi agli accessi potranno essere conservati per un periodo non superiore ad una settimana con la predisposizione di specifici meccanismi di integrale cancellazione automatica delle informazioni allo scadere del termine previsto. L'accesso ai dati infine potrà essere garantito ai soli interessati oppure all'autorità giudiziaria ove specificamente richiesto.

## L'attività del Garante. Per chi vuole saperne di più

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

- Bollette telefoniche: anche le ultime tre cifre potranno essere "in chiaro" - Comunicato del 1.4.2008
- Ragazza inglese uccisa: il Garante chiede registrazione programma - Comunicato del 1.4..2008
- Avvio consultazione pubblica sullo schema preliminare del Codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria - 4.4. 2008
- A Roma l'annuale conferenza dei Garanti europei della privacy - Comunicato del 17.4.2008
- Su controllo delle frontiere e circolazione dei viaggiatori, i Garanti privacy europei chiedono maggiori garanzie - Comunicato del 18.4.2008

### 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](http://www.garanteprivacy.it)