
Privacy - Newsletter del Garante n. 335 del 1° marzo 2010 (traffico tlc e Internet, diritto di cronaca, RFID, futuro privacy)

By Panfilo Marcelli

Published: 01/03/2010 - 16:33

Il Garante per la protezione dei dati personali ha pubblicato la [newsletter n. 335 del 1° marzo 2010](#). Quattro gli argomenti trattati:

1. Dati di traffico tlc e Internet: no a conservazione illimitata
2. Violenza sessuale e diritto di cronaca
3. Nuove tecnologie e aree a rischio
4. Il futuro della privacy

Di seguito il testo integrale della newsletter.

Dati di traffico tlc e Internet: no a conservazione illimitata

Gestori telefonici e internet provider di nuovo sotto la lente del Garante privacy. L'Autorità ha vietato [doc web n. [1695393](#), [1695368](#) e [1683093](#)] a tre società che operano nel settore della telefonia e Internet l'uso di dati trattati in modo illecito e ne ha ordinato la cancellazione. Tempi di conservazione dei dati di traffico telefonico e telematico superiori al consentito e conservazione di informazioni sui siti visitati dagli utenti alcune delle gravi violazioni emerse nel corso degli accertamenti ispettivi effettuati dall'Autorità.

I dati di traffico telefonico (numero chiamato, data, ora, durata della chiamata, localizzazione del chiamante in caso di cellulare ecc.) e Internet (indirizzi e-mail contattati, data, ora, durata degli accessi alla rete ecc.) non riguardano il contenuto della comunicazione, ma sono comunque particolarmente delicati poiché consentono di ricostruire tutte le relazioni di una persona e le sue abitudini.

Le società dovranno innanzitutto cancellare i dati di traffico telefonico e telematico conservati oltre i tempi previsti dalla normativa italiana per finalità di accertamento e repressione dei reati (ventiquattro mesi per i dati di traffico telefonico; dodici mesi per i dati telematici). In un caso, i dati di traffico telefonico risalivano addirittura a marzo 1999 e quelli di traffico telematico a giugno 2007. Da cancellare anche tutte le informazioni in grado di rivelare gusti, opinioni, tendenze degli utenti che non avrebbero mai dovuto essere archiviate nei data base (ad esempio, l'oggetto dei messaggi di posta elettronica inviati e ricevuti; i dati personali relativi alla navigazione in Internet, anche quando rappresentati dal solo indirizzo Ip di destinazione). Ad una società è stato prescritto di innalzare i livelli di sicurezza dei flussi informativi con l'autorità giudiziaria e di garantire in modo più adeguato la riservatezza delle informazioni: al posto del fax dovranno essere adottati sistemi di comunicazione

sviluppati con protocolli di rete sicuri e strumenti di cifratura basati su firma digitale. Gli accertamenti disposti dal Garante rientrano nell'ambito di un'azione comune deliberata dalle Autorità di protezione dei dati europee riunite nel Gruppo di lavoro art. 29 e sono volti a verificare l'osservanza, da parte dei fornitori di servizi di comunicazione elettronica, degli obblighi fissati dalla normativa nazionale in materia di conservazione dei dati di traffico. I fornitori sono stati individuati sulla base di diversi criteri (quota di mercato, tipologia dei servizi forniti, dimensione nazionale o internazionale)

Violenza sessuale e diritto di cronaca

Gli organi di informazione non possono pubblicare i nomi dei violentatori se ciò rende identificabili le vittime dell'abuso sessuale. E non ha alcun rilievo il fatto che le informazioni siano di dominio pubblico perché già diffuse da altre testate giornalistiche o perché divulgate da magistrati e forze di polizia in una conferenza stampa. Alle vittime di violenza sessuale è sempre riconosciuta una tutela assoluta. Sono queste le motivazioni alla base del [divieto](#) deciso dal Garante privacy (relatore Mauro Paissan) nei confronti di alcune agenzie di stampa e di alcuni quotidiani che non potranno più pubblicare informazioni lesive della riservatezza e della dignità di una minore. Quelle informazioni dovranno essere cancellate anche dalle edizioni online. Nel riportare la notizia di una violenza sessuale in famiglia avvenuta in provincia di Salerno, queste testate avevano infatti pubblicato nome, cognome, professione, età del padre, del fratello e di un vicino di casa arrestati quali presunti autori del reato. In questo modo, pur senza fare espressamente il nome della vittima, avevano diffuso informazioni così dettagliate da renderla riconoscibile. Ciò in aperto contrasto con i principi fissati dal Codice deontologico dei giornalisti, dalla normativa italiana e dalle Convenzioni internazionali (Codice privacy, Codice penale, nuovo processo minorile, Carta di Treviso, Convenzione dei diritti del fanciullo) che riconoscono una tutela rafforzata alle vittime minori d'età. Il divieto del Garante fa seguito a un primo [provvedimento di blocco](#), adottato in via d'urgenza, al momento della pubblicazione della notizia.

Copia del provvedimento di divieto è stata inviata alla Procura della repubblica e ai Consigli regionali dei giornalisti di competenza.

Nuove tecnologie e aree a rischio

Si dell'Autorità a sistemi integrati per garantire la sicurezza degli accessi

Il Garante privacy [ha autorizzato](#) un consorzio di aziende che commercializza preziosi a utilizzare un sistema di sicurezza basato sulla rilevazione delle impronte digitali combinata con una tecnologia di riconoscimento a radiofrequenza (Rfid).

A sostegno della sua richiesta, il centro orafa aveva addotto motivi di sicurezza derivanti dall'enorme estensione della struttura e dalla sua collocazione in un'area industriale ad alto tasso di criminalità. Il progetto sottoposto a verifica preliminare del Garante, prevede per l'accesso alla struttura un sistema di doppie porte automatiche e l'utilizzo di una smart card, in esclusiva dotazione di dipendenti e fornitori, in cui è inserito un codice alfanumerico ricavato dall'impronta digitale.

In prossimità della prima porta, un sistema a radiofrequenza (Rfid) "legge" la smart card e verifica le credenziali d'accesso e il codice ricavato dall'impronta. Superata la prima porta, un lettore biometrico accerta la corrispondenza tra l'impronta di chi sta entrando e il codice registrato. I dati rilevati vengono

immediatamente cancellati.

L'Autorità ha ritenuto proporzionato e conforme alla disciplina privacy il sistema proposto, anche tenendo conto degli effettivi problemi di sicurezza del complesso orafa. Ha tuttavia prescritto all'azienda una serie di obblighi, tra i quali quello di non

utilizzare il sistema per finalità diverse (come ad esempio il controllo dell'orario di lavoro) e di fornire agli interessati un'informativa in cui vengano chiarite le modalità alternative di accesso al centro per chi non possa o non intenda usufruire del sistema biometrico. Dovranno essere inoltre predisposte misure idonee per inibire tempestivamente l'uso delle smart card in caso di smarrimento o furto.

Il futuro della privacy

Il Gruppo dei Garanti europei (Gruppo "Articolo 29") e il Gruppo di lavoro "polizia e giustizia" (Working Party on Police and Justice), presieduto da Francesco Pizzetti, presidente dell'Autorità italiana, hanno messo a punto congiuntamente un documento per rispondere alla consultazione pubblica che la Commissione europea ha aperto lo scorso anno sul futuro della protezione dei dati. Il contributo è disponibile sul sito del Gruppo Articolo 29 (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf).

Il punto di vista delle Autorità europee per la protezione dei dati è che l'impianto normativo di base assicurato dalla Direttiva del 1995 resta valido. E' tuttavia auspicabile che il legislatore europeo introduca alcune innovazioni e modifiche per rendere ancora più effettivo il diritto fondamentale alla protezione dei dati, ormai parte integrante del Trattato di Lisbona. Secondo le Autorità garanti è necessario che i diritti di cui godono gli interessati siano esercitabili in modo semplice ed efficace, facilitando l'accesso a rimedi di natura giudiziaria (ad esempio attraverso l'introduzione di "class action") e favorendo il ricorso a sistemi alternativi per la risoluzione delle controversie. I Garanti europei propongono anche l'introduzione dell'obbligo giuridico per chi tratta i dati di dimostrare di avere adottato tutte le misure previste dalla legge, trasformando la protezione dei dati in un elemento intrinseco e portante dell'organizzazione interna. Più in generale, i Garanti ritengono necessario che i principi alla base della Direttiva 95/46 e di tutte le direttive ad essa connesse (come la direttiva e-privacy, la n.2002/58) divengano parte integrante delle tecnologie secondo un approccio detto comunemente di "privacy by design".

Largo spazio viene dedicato nel documento alle attività di cooperazione fra le Autorità di protezione dati, con particolare riguardo alle "sfide" che attendono la protezione dati nell'area del cosiddetto "Terzo pilastro". In questi ultimi anni, la cooperazione in materia giudiziaria e di polizia ha visto un incredibile potenziamento degli strumenti giuridici e tecnici finalizzati a consentire scambi di dati ed intelligence sempre più pervasivi ed estesi, senza che a ciò si accompagnasse un ripensamento ed un'armonizzazione degli strumenti e delle norme a tutela della sfera privata dei cittadini. Su questo punto i Garanti Ue chiedono ai legislatori europei e nazionali di invertire la tendenza, sviluppando un quadro giuridico uniforme, come previsto del resto anche nel "programma di Stoccolma" presentato dal Consiglio europeo dello scorso dicembre, in modo da muoversi nell'ottica del Trattato di Lisbona.

Chi è Panfilo Marcelli?

L'ingegner Panfilo Marcelli ha lavorato per oltre vent'anni presso primarie aziende informatiche e di consulenza (IPACRI, Euros Consulting, OASI) con incarichi, anche direttivi, in ambito Information Technology, Privacy e Protezione dei dati personali, Qualità e Certificazione ISO9000 e ISO27001, Workflow Management e Business Process Reengineering, Internet, Intranet e gestione di siti con sistemi CMS. Attualmente è socio di CMA Consulting società specializzata in servizi, consulenza e formazione in ambito Compliance, Privacy, Qualità e Sicurezza. □

Panfilo Marcelli cura gli articoli dedicati alla "Privacy" sul sito www.ComplianceNet.it ed è l'autore dell'ebook "Sei lezioni sulla privacy".

Ultimi articoli di Panfilo Marcelli

- [Privacy - Newsletter del Garante n. 334 dell'11 febbraio 2010 \(Carte di credito, Certificati medici, Archivi Schengen, Ue-Usa\)](#)

-
promulgate nel marzo 2009">Privacy: il Garante ribadisce le regole sul telemarketing già promulgate nel marzo 2009

- [Analisi mediche via mail. Le regole del Garante privacy](#)

- [Privacy: linee guida in tema di referti on-line](#)

- [Amministratori di sistema: precisazioni del Garante](#)

- [Privacy - Newsletter del Garante n.332 del 10 dicembre 2009](#)

protezione dei dati personali – cambia tutto">Privacy e telemarketing : aggiornato il Codice in materia di protezione dei dati personali – cambia tutto

-
comunicazioni infragruppo">Privacy e antiriciclaggio: provvedimento del Garante sulle comunicazioni infragruppo

-
perplexità e preoccupazione">Telemarketing: su nuove norme il Garante privacy esprime perplexità e preoccupazione

- [Acquista "Sei lezioni sulla privacy" su miolibro.it](#)