



- INVESTIGATORI PRIVATI, BANCHE, CLOUD COMPUTING SOTTO LALENTE DEL GARANTE
- VIOLAZIONE DELLA PRIVACY NELL'AMBITO DEI PROCESSI: L'ULTIMA PAROLA AL GIUDICE
- CREDITO AL CONSUMO: ACCESSO AI DATI PER I FINANZIATORI UE
- TRASPORTO: IMPRONTE DIGITALI SOLO IN CASI PARTICOLARI

## Investigatori privati, banche, cloud computing sotto la lente del Garante

Varato il piano ispettivo per il primo semestre 2011. Nello scorso anno applicate sanzioni per circa 3 milioni e 800 mila euro

Investigatori privati, servizi informatici (in particolare quelli forniti mediante il cosiddetto "cloud computing"), istituti bancari e carte di credito, marketing (anche via sms ed e-mail), enti previdenziali.

E' su questi delicati settori e sulle modalità con le quali vengono trattati i dati personali di milioni di cittadini italiani che si concentrerà l'attività di accertamento del Garante per la privacy nei primi sei mesi dell'anno. Il piano ispettivo appena varato prevede specifici controlli, sia nel settore pubblico che in quello privato, anche riguardo alle informazioni da fornire ai cittadini sull'uso dei loro dati personali, all'adozione delle misure di sicurezza, alla durata di conservazione dei dati, al consenso da richiedere nei casi previsti dalla legge, all'obbligo di notificazione al Garante. Oltre 250 gli accertamenti ispettivi programmati che verranno effettuati come di consueto anche in collaborazione con le Unità Speciali della Guardia di Finanza - Nucleo Privacy. A questi accertamenti si affiancheranno quelli che si renderanno necessari in ordine a segnalazioni e reclami presentati.

Intanto, un primo bilancio sull'attività ispettiva relativa al 2010 mostra il significativo lavoro di controllo svolto dall'Autorità: sono state circa 474 le ispezioni effettuate e 424 i procedimenti sanzionatori, relativi in larga parte alla omessa informativa, al trattamento illecito dei dati, alla mancata adozione di misure di sicurezza, all'inosservanza dei provvedimenti del Garante.

Le ispezioni hanno riguardato in particolare il settore sanitario, le catene alberghiere, l'attivazione di schede telefoniche multiple, la formazione on line.

Le segnalazioni all'autorità giudiziaria per violazioni penali sono state 55, e hanno riguardato tra l'altro la mancata adozione delle misure di sicurezza, la falsità

nelle dichiarazioni e nelle notificazioni, il mancato adempimento ai provvedimenti del Garante. Complessivamente le entrate derivanti dalle sanzioni sono state pari a circa 3 milioni e 800 mila euro: in particolare, 2 milioni relativi alle violazioni degli obblighi sull'informativa, 800 mila relativi al trattamento illecito di dati e 450 mila relativi alla mancata adozione di misure di sicurezza da parte di aziende e pubbliche amministrazioni.

## Violazione della privacy nell'ambito dei processi: l'ultima parola al giudice

Spetta al giudice la valutazione sull'utilizzabilità degli atti prodotti dagli avvocati o dalle parti

Spetta al giudice, e non al Garante della privacy, la valutazione sulla liceità del trattamento dei dati personali anche effettuato dagli avvocati o dalle parti nel corso del processo e di conseguenza la utilizzabilità o meno degli atti e dei documenti da loro prodotti. Tale chiarimento trae origine da due segnalazioni e un reclamo pervenuti all'Autorità da parte di cittadini che si lamentavano per l'utilizzo di dati sensibili e giudiziari a loro riferiti. In un caso, nell'ambito di una causa di separazione, venivano contestate le modalità di acquisizione e l'utilizzabilità di alcune lettere private contenenti dati idonei a rivelare la vita sessuale della reclamante. Un'altra contestazione era riferita all'utilizzabilità, all'interno di una causa di lavoro, di dati relativi a una vicenda giudiziaria penale. L'ultima segnalazione riguardava la produzione di una e-mail contenente informazioni sullo stato di salute, presentata in un contenzioso civile tra due società.

In tutti e tre i provvedimenti l'Autorità ha sottolineato che, in base all'articolo 160 del Codice della Privacy, spetta al giudice definire la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti presentati o acquisiti nell'ambito del procedimento giudiziario, anche se basati su un trattamento illecito di dati personali. Tale valutazione è infatti disciplinata dalle

pertinenti disposizioni processuali in materia civile e penale.

## Credito al consumo: accesso ai dati per i finanziatori Ue

Il Garante per la protezione dei dati personali ha dato il via libera allo schema di delibera del Comitato interministeriale per il credito ed il risparmio (CICR) con il quale viene prevista la possibilità per gli istituti di credito e le società finanziarie degli Stati membri dell'Ue di accedere alle banche dati italiane, pubbliche e private, contenenti informazioni sul credito.

Lo schema di delibera, dando attuazione alla direttiva europea in materia, consente infatti ai finanziatori operanti nell'ambito dell'Unione europea di accedere ai Sic (Sistemi di informazione creditizie) e alla centrale rischi della Banca d'Italia in condizioni "non discriminatorie" rispetto a quelle previste per i finanziatori italiani (in particolare per quanto riguarda i costi, le qualità del servizio di accesso ai dati, le modalità per la sua fruizione e la tipologia di informazioni fornite). Lo schema prevede inoltre che venga salvaguardato il "principio di reciprocità", su cui si fondano le banche dati sul credito operanti in Italia, in base al quale l'accesso è consentito soltanto ai finanziatori che forniscono a loro volta le informazioni creditizie in loro possesso.

Il parere è stato reso dal Garante su una versione aggiornata dello schema di delibera che tiene conto degli approfondimenti e delle indicazioni fornite dalla stessa Autorità agli uffici della Banca d'Italia allo scopo di garantire un più elevato standard di tutela del diritto alla protezione dei dati personali. Sulla base delle osservazioni dell'Autorità sono stati infatti meglio chiariti in particolare due aspetti: la finalità dell'accesso, che deve essere unicamente la valutazione del "merito creditizio" del consumatore, e i soggetti cui possono riferirsi le informazioni, vale a dire esclusivamente il consumatore ed i "soggetti col medesimo coobbligati anche in solido", in linea con quanto previsto dal Codice di deontologia sui sistemi informativi in tema di credito al consumo.

## Trasporto: impronte digitali solo in casi particolari

Occorre dimostrare che non sono sufficienti strumenti alternativi

Le imprese che intendono adottare sistemi di lettura delle impronte digitali per verificare la presenza in servizio dei dipendenti devono prima dimostrare che le finalità di controllo non possano essere realizzate con sistemi meno invasivi. Questa la decisione Garante che ha respinto le richieste di verifica preliminare con le quali due società - una impresa di autotrasporti e la sua capogruppo - chiedevano di poter usare un meccanismo di autenticazione biometrico.

NEWSLETTER

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

In base alla documentazione presentata, tale procedura avrebbe dovuto riguardare in primo luogo i lavoratori addetti al controllo degli automezzi e del personale di guida. Secondo le società, il rilevamento delle impronte avrebbe evitato eventuali condotte irregolari, come lo scambio di badge attestanti la presenza in servizio, e avrebbe di conseguenza determinato anche maggiori garanzie per l'incolumità degli utenti e del personale viaggiante. Nel corso dell'istruttoria è però emerso che i tradizionali metodi di controllo si erano dimostrati più che sufficienti a garantire la verifica della presenza in servizio dei dipendenti, evidenziando la mancata necessità di introdurre sistemi così invasivi. L'uso dei sistemi biometrici era stato richiesto dalle due società anche per accedere ai locali dove sono custoditi le banche dati cartacee e informatiche contenenti i dati personali dei dipendenti. Anche in questo caso, dagli accertamenti effettuati dal Garante è però emerso che tali dati non richiedevano particolari sistemi di controllo, trattandosi di informazioni solitamente elaborate dagli uffici amministrativi di qualsiasi azienda.

Nei provvedimenti con i quali ha respinto la richiesta delle due società di autotrasporti, l'Autorità ha ritenuto opportuno sottolineare che l'utilizzo di sistemi di riconoscimento basati su dati biometrici è possibile solo in casi particolari, per i quali sia dimostrato che non siano sufficienti strumenti alternativi e che dunque la raccolta delle impronte digitali risulti davvero necessaria e proporzionata.

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

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

Linee guida sulla diffusione on line di documenti e informazioni da parte delle pubbliche amministrazioni -  
Avvio consultazione - Comunicato del 22.12. 2010

Proroga l'autorizzazione al trattamento dei dati genetici -  
Comunicato del 30.12.2010

Garante privacy: al via le Linee guida per l'informazione giuridica - Comunicato 3.1.2011

Tessera del tifoso: più garanzie per i supporter -  
Comunicato del 12.1.2011

Garante privacy: i media valutino interesse pubblico delle notizie - Comunicato 17.1.2011

Caso Ruby: Garante a siti web e media, oscurate i numeri telefonici - Comunicato del 21.1.2011

Telemarketing: le regole del Garante per l'uso dei dati degli abbonati - Comunicato del 31.1.2011

Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n.121 - 00186 Roma.  
Tel: 06/696772751 - Fax: 06/696773755. Newsletter è consultabile sul sito Internet [www.garanteprivacy.it](http://www.garanteprivacy.it)

