



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Newsletter

NOTIZIARIO SETTIMANALE
ANNO XV
WWW.GARANTEPRIVACY.IT

NEWSLETTER N. 394 del 16 ottobre 2014

- [Sì ai Big Data nelle statistiche nazionali, ma occorrono garanzie](#)
- ["Internet delle cose": Garanti privacy Ue, serve un approccio etico](#)
- [Niente spam per gli iscritti alla newsletter](#)
- [Magazzini videosorvegliati più a lungo: ok del Garante](#)

Sì ai Big Data nelle statistiche nazionali, ma occorrono garanzie

I Big Data entrano nelle statistiche nazionali. Il Garante ha dato [parere favorevole](#) sullo schema di Programma statistico nazionale 2014-2016 Aggiornamento 2015-2016 (Psn), predisposto dall'Istat, che prevede, tra l'altro, la possibilità di utilizzare per la prima volta a fini statistici, seppur in via sperimentale, i Big Data di telefonia mobile. Tale elaborazione statistica ha l'obiettivo di effettuare una stima a livello aggregato dei flussi di mobilità intercomunali delle persone, utile per la programmazione e la gestione dei servizi locali e l'individuazione di opportune misure di Protezione civile. L'Autorità ha però richiesto precise garanzie a tutela degli interessati.

I Big Data rappresentano, infatti, un enorme patrimonio informativo e l'utilizzo di queste informazioni comporta specifici rischi per la tutela della riservatezza degli interessati, tenuto conto anche del fatto che, grazie alle nuove tecnologie e alle nuove tecniche di analisi ed elaborazione, interconnessione dei dati, risulta possibile "re-identificare" un interessato attraverso informazioni apparentemente

anonime.

Il progetto in esame prevede che l'Istat tratti dati relativi al cosiddetto "call detail record" (cdr). Il cdr è un numero progressivo, assegnato dal gestore telefonico all'utente che effettua la chiamata (in sostituzione del codice fiscale, nome e cognome), al quale vanno aggiunte le informazioni relative al Comune nel quale si trova la cella di effettuazione, la data e l'ora della chiamata. Gli utenti verranno distinti in quattro categorie: residenti stanziali, temporaneamente dimoranti, pendolari giornalieri e visitatori occasionali.

Riguardo all'uso di questi dati, su specifica richiesta del Garante, l'Istat ha fornito idonee garanzie sul fatto che presso il gestore siano raccolti solo dati in forma anonima. E' stato previsto infatti che il gestore assegni un codice ad ogni cdr e che successivamente venga eliminata ogni possibilità di raccordo tra tale codice e gli identificativi originali.

E' emersa, inoltre, l'esigenza di porre particolare attenzione anche alle successive modalità di trattamento dei dati anonimi raccolti dall'Istat presso i gestori telefonici. In particolare, con riferimento al rischio di individuare una unità elementare, derivante dal collegamento dei dati con altri data base in possesso dell'Istat, il Garante ha specificamente richiesto che vengano oscurate frequenze di flusso inferiori a tre unità.

La raccolta dei dati di telefonia mobile riguarderà al momento solo la provincia di Pisa e i soli dati del mese di ottobre 2011, e verrà effettuata a fini di sperimentazione e messa a punto di applicativi per la stima di flussi aggregati. Con riferimento a tale attività, l'Autorità si è riservata, infine, di effettuare specifiche verifiche anche in relazione ai trattamenti svolti dai gestori telefonici.

"Internet delle cose": Garanti privacy Ue, serve un approccio etico

Un approccio "etico" all'Internet delle cose. E' il messaggio che i Garanti per la privacy europei hanno lanciato con un recente parere dedicato alla crescente diffusione di dispositivi "intelligenti" che sono in grado di interagire creando una rete di monitoraggio e controllo spesso del tutto invisibile per gli utenti.

Il proliferare di tecnologie che promettono di semplificarci la vita (dalla domotica al monitoraggio delle condizioni bio-fisiche, fino all'uso di sensori impiantabili nel corpo umano) genera evidenti rischi per la vita privata delle persone. Per questo motivo i Garanti europei hanno fornito indicazioni e raccomandazioni a tutti gli stakeholder volte ad innalzare il livello di protezione dei dati di milioni di persone.

Il documento (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf) si sofferma, in particolare, su tre settori in grande sviluppo, caratterizzati da un legame diretto, quasi fisico, con l'individuo: quelli del *wearable computing* (abiti, accessori ed altri dispositivi, quali occhiali, indossabili dalle persone), del *quantified self* (sensori ed altri dispositivi utilizzati per misurazioni di prestazioni o condizioni corporee) e della domotica (il "frigorifero intelligente", la "casa intelligente").

Asimmetria informativa (gli utilizzatori spesso non sanno quali dati siano raccolti, né chi in ultima analisi vi possa accedere), profilazione potenzialmente illimitata di abitudini e comportamenti, rischi per la sicurezza dei dati che possono essere raccolti e incrociati attraverso gli oggetti interconnessi: sono questi i principali lati oscuri dell'Internet delle cose, secondo le Autorità europee. Per ciascuno di essi vengono indicate utili contromisure e raccomandazioni, rivolte a tutti gli stakeholder interessati: produttori, sviluppatori di app, piattaforme social. I Garanti chiedono, in primo luogo, che il maggior numero di garanzie siano introdotte già nella fase progettuale: ciò si traduce nell'applicazione dei principi di "privacy by design" e "privacy by default" e nell'adozione coerente del principio di minimizzazione dei dati personali.

In secondo luogo, all'utilizzatore deve rimanere il controllo dei dati trattati dall'"oggetto" in ogni fase (ad esempio, sia mediante protocolli informatici "*privacy friendly*", sia mediante l'adozione di interfacce utente di facile uso). Nel caso in cui il consenso sia la base giuridica per il trattamento, deve trattarsi di un consenso informato, libero e specifico.

Particolare cura dovrà essere riservata alle informative, che dovranno essere chiare e dettagliate, anche da parte delle molte app che già offrono molteplici funzionalità, basate sulla raccolta di dati (anche biometrici e sensibili) attraverso sensori e dispositivi intelligenti. Inoltre, occorrerà valutare attentamente i requisiti (anche di sicurezza) che i singoli sviluppatori devono soddisfare.

Non secondario, infine, il contributo che secondo i Garanti per la privacy Ue gli organismi di standardizzazione (ISO, CEN, ecc.) possono e devono dare in questo ambito per individuare protocolli e sistemi comuni, soprattutto con l'obiettivo di fornire agli utilizzatori la garanzia di un'applicazione efficace dei principi di protezione dati e di sicurezza.

Niente spam per gli iscritti alla newsletter

Illecito il comportamento di una società che inviava email promozionali senza

consenso

Un cittadino che compila un form on line per ricevere una newsletter deve poter decidere, liberamente e consapevolmente, se dire sì o no alle comunicazioni promozionali, alla profilazione, all'invio dei suoi dati ad altre società e, in generale, a tutti i tipi di trattamenti che vanno al di là del servizio richiesto. La registrazione alla newsletter, inoltre, non può essere condizionata al rilascio del consenso anche per altre finalità.

Il principio è stato ribadito dal Garante privacy che [ha vietato](#) l'uso dei dati a fini commerciali ad una società che inviava e-mail promozionali senza consenso agli utenti registrati a un servizio di newsletter. Ora la società, destinataria del provvedimento inibitorio dell'Autorità, potrà utilizzare i dati fin qui raccolti solo per inviare la newsletter. Se vorrà inviare email promozionali dovrà mettersi in regola con il Codice della privacy, modificando il form di registrazione in modo da consentire agli utenti la possibilità di esprimere, un preventivo consenso "ad hoc" per la ricezione di email promozionali. Dagli accertamenti svolti dall'Ufficio del Garante su segnalazione di un cittadino che lamentava la ricezione di pubblicità indesiderata, è emerso infatti che per iscriversi la newsletter l'utente, al momento di inserire nel form on line l'indirizzo email, poteva esprimere solo un generico, omnicomprendente consenso al "trattamento dei dati personali". L'accesso al servizio era, peraltro, condizionato alla manifestazione di tale generico consenso. Il comportamento della società è stato dichiarato illecito dal Garante perché i trattamenti di dati per fini commerciali esulano da quelli necessari per adempiere al contratto di fornitura di un servizio. L'Autorità sta valutando, con separato provvedimento, l'applicazione della sanzione amministrativa per l'illecito commesso.

Magazzini videosorvegliati più a lungo: ok del Garante

Una società di trasporti internazionali potrà estendere fino a 90 giorni i tempi di conservazione delle immagini videoregistrate nei magazzini delle proprie filiali, ma solo per consentire l'accertamento di eventuali illeciti e l'individuazione dei possibili responsabili da parte dell'autorità giudiziaria.

Lo [ha stabilito](#) il Garante privacy accogliendo l'istanza di verifica preliminare presentata dalla società al fine di rafforzare il livello di tutela dei beni aziendali e della merce stoccata nei propri magazzini, di prevenire furti o manomissioni delle merci custodite e di garantire la qualità del servizio.

L'ok del Garante all'estensione dei tempi di conservazione delle immagini tiene

conto, tra l'altro, delle specifiche modalità di lavoro della società le quali prevedono che le merci, essendo spesso oggetto di trasporti internazionali, possano giungere a destinazione diversi giorni dopo lo stoccaggio in magazzino. Di conseguenza, in alcuni casi le eventuali manomissioni risultano rilevabili solo dopo molto tempo dalla spedizione, attraverso una ricostruzione delle cause che può richiedere l'analisi di immagini registrate anche molti giorni prima. Le esigenze di una videosorveglianza più lunga, inoltre, sono collegabili alle stringenti norme internazionali sulla sicurezza dei trasporti di persone e merci che prevedono standard molto elevati e alle procedure di controllo doganale cui la società è soggetta. Operando attraverso i depositi doganali, la società è infatti obbligata a trattenere presso i propri magazzini le merci che l'Autorità doganale intende sottoporre a controlli più approfonditi e quelle sulle quali vi siano sospetti di reato relativi alle spedizioni.

L'ATTIVITÀ DEL GARANTE - PER CHI VUOLE SAPERNE DI PIÙ

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

- [Call center: da oggi stop alle "telefonate mute"](#) - Comunicato del 2 ottobre 2014
- [Pubblicazione integrale sul web delle sentenze pronunciate dalla Corte di Cassazione e protezione dei dati personali - Lettera di Antonello Soro a Giorgio Santacroce, Primo Presidente della Corte suprema di Cassazione](#) - 6 ottobre 2014

NEWSLETTER

del Garante per la protezione dei dati personali (Reg. al Trib. di Roma n. 654 del 28 novembre 2002).

Direttore responsabile: Baldo Meo.

Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n. 121 - 00186 Roma.

Tel: 06.69677.2752 - Fax: 06.69677.3755

Newsletter è consultabile sul sito Internet www.garanteprivacy.it