TLS Newsletter

Mercoledì 20 luglio 2016

Per maggiori informazioni: info.tls@it.pwc.com

Relazione sull'attività del Garante per l'anno 2015

di Stefano Cancarini e Flavia Messina

Ogni anno, nel mese di giugno, l'Autorità Garante per la protezione dei dati personali pubblica una Relazione con l'indicazione delle principali attività svolte e le decisioni adottate nel corso dell'anno precedente.

Anche quest'anno, in data 28 giugno 2016, il Garante ha pubblicato la relazione relativa al 2015. Di seguito un *focus* su alcuni interventi di particolare interesse.

Innanzitutto, l'Autorità nel 2015 ha condotto 303 ispezioni concentrate, tra le altre, sulle seguenti realtà: ospedali ed aziende sanitarie; società che effettuato attività di marketing telefonico mediante call center operanti all'estero; società che gestiscono sistemi di pagamento su dispositivi portatili; banche; operatori telefonici e società che forniscono servizi finalizzati alla fidelizzazione della clientela. Contestualmente sono stati avviati 1.696 nuovi procedimenti sanzionatori amministrativi.

Nel presentare una stima di quelle che sono state le violazioni maggiormente ripetutesi nel corso del 2015, il Garante ha evidenziato la mancata acquisizione del consenso dell'interessato, violazione che si è verificata in 1.270 dei casi esaminati dall'Autorità. In totale, le sanzioni amministrative riscosse ammontano ad Euro 3.345.515.

In relazione alle istruttorie effettuate, il Garante ha, inoltre, inviato 33 segnalazioni di **violazioni penali** all'autorità giudiziaria. Oggetto di tali segnalazioni sono state, per lo più, la mancata adozione delle misure minime di sicurezza, la violazione dello Statuto dei lavoratori (L. n. 300/1970), la falsità nelle dichiarazioni e notificazioni al Garante, il trattamento illecito dei dati e l'inosservanza di un provvedimento del Garante.

Italian Data Protection Authority - Annual Report 2015

On June 28, 2016, the Italian Data Protection Authority issued its annual report summarizing the main activities and decisions undertaken during the previous year. In such respect, the key areas on which the Authority focused its attention during 2015 were: the processing of personal data for marketing purposes; the Internet of Things and mobile ticketing, on which the Authority launched two public consultations; the health care sector, with the issuance of the Guideline on the Health File; as well as the banking and insurance sectors. With respect to the investigations carried out in 2015, the Authority revealed that the administrative sanctions paid for the violation of the Privacy Code were equal to Euro 3,345,515.

In tale contesto, particolare risonanza è stata data dall'Autorità per la protezione dei dati ai casi di mancata adozione delle misure minime di sicurezza, descritti come adempimenti "*di non particolare complessità, in vigore da più di dieci anni, che dovrebbero essere stati ormai metabolizzati sia dalle imprese che dagli enti pubblici*" e che, esponendo i dati personali degli interessati all'accesso da parte di persone non autorizzate, intaccano il naturale affidamento degli interessati nei confronti del titolare del trattamento.

Coerentemente con la riforma del quadro normativo europeo che ha tenuto conto della rivoluzione digitale in atto negli ultimi anni, una larga parte delle attività del Garante ha avuto ad oggetto il trattamento dei dati personali attraverso Internet. In tale contesto, l'Autorità si è pronunciata relativamente al **trattamento dei dati per finalità di *marketing***, ribadendo l'obbligo in capo al titolare del trattamento, in primo luogo, di fornire un'informativa chiara, completa e facilmente accessibile e, in secondo luogo, qualora i dati siano utilizzati al fine di definire il profilo dell'utente e/o di promozione commerciale, di ottenere dagli interessati specifici consensi, revocabili in qualsiasi momento, per ciascuna distinta finalità di trattamento.

Inoltre, sulla scia di quanto già indicato con riferimento all'uso dei cookies, al fine di rendere più agevole il rilascio del consenso, il Garante ha ipotizzato l'utilizzo di un *banner* attraverso il quale mettere l'utente in condizione di effettuare scelte consapevoli sul trattamento dei dati che lo riguardano.

In tale ambito, inoltre, a seguito di alcune richieste di verifica preliminare promosse da operatori telefonici da un lato, e soggetti operanti nel settore delle carte fedeltà dall'altro, il Garante ha individuato alcuni accorgimenti, tra cui, specifiche misure di sicurezza da adottare per il trattamento di dati aggregati della clientela ai fini della composizione dei cluster di utenti, nonché indicazioni inerenti al tempo di conservazione dei dati.

In vista dell'ampliarsi del fenomeno, il Garante ha avviato una consultazione pubblica al fine di acquisire elementi e proposte relativamente all'**Internet delle cose** (insieme di tecnologie che, per il mezzo di sensori integrati negli oggetti, consentono di "*registrare, processare, immagazzinare dati localmente o tramite l'interoperabilità dei dispositivi tra loro*"). Oltre che sulla possibilità di acquisire un eventuale consenso dell'interessato, la consultazione aveva ad oggetto, la possibilità di adottare soluzioni tecnologiche a garanzia della *privacy* fin dalla progettazione (in un'ottica di c.d. *privacy by design*), la possibilità di adottare tecniche di cifratura ed anonimizzazione. La procedura di consultazione si è conclusa nel dicembre 2015, attendendosi per i prossimi mesi i provvedimenti di valutazione della consultazione da parte dell'Autorità.

Con riferimento al c.d. ***mobile ticketing*** (*i.e.* servizi di pagamento attraverso il telefono cellulare), il Garante, riservandosi di intervenire con provvedimenti puntuali sul tema, ha annunciato una consultazione pubblica in proposito.

Particolare risalto nel 2015 è stato dato dal Garante anche al settore della sanità elettronica con l'emanazione delle **Linee guida in materia di *dossier* sanitario elettronico**. Al riguardo, l'Autorità ha ribadito la necessità di riconoscere agli interessati ampia libertà circa la possibilità di far costituire o meno il *dossier*, nonché chiare informazioni in merito ai soggetti che possono avere accesso ai propri dati e delle operazioni che possono svolgere con riferimento agli stessi. Il Garante in tale circostanza, ha precisato che, in assenza del consenso, il medico avrà a disposizione solo le informazioni rese di volta in volta dal paziente o fornite allo stesso professionista in occasione di visite precedente.

Centrale è stato anche il tema della notificazione dei ***data breach***, che ha recentemente ricevuto grande attenzione con riferimento al nuovo Regolamento europeo che ne ha ampliato l'ambito di applicazione. Indipendentemente dall'ambito del trattamento, ha poi precisato che la quasi totalità dei casi notificati ha riguardato eventi che hanno coinvolto un numero di interessati inferiore a 100 e solo in 4 casi la violazione ha avuto una portata più ampia (oltre 2.000,00 soggetti coinvolti).

In ambito bancario parte delle verifiche dell'Autorità sono state indirizzate all'implementazione delle prescrizioni contenute nella decisione in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie, adottata dal Garante con provvedimento n. 192 del 12 maggio 2011. Il Garante ha, inoltre, avviato i lavori per apportare modifiche al codice deontologico SIC (Sistema di Informazioni Creditizie), individuando le tematiche da approfondire e la metodologia da seguire.

Con riferimento all'ambito assicurativo e, in particolare, alla banca dati degli attestati di rischio, il Garante ha rilasciato il proprio parere favorevole su uno schema di regolamento dell'IVASS a condizione che vengano previste specificazioni riguardo le finalità sottese alla trasmissione delle informazioni, le misure di sicurezza, l'informativa e il consenso, nonché un termine massimo per la conservazione dei dati.

Significativa è stata anche l'attività condotta dal Garante a livello internazionale. La *privacy* è stata negli ultimi tempi al centro di numerosi dibattiti e protagonista di eventi di particolare rilievo. Tra tutte, nell'ottobre del 2015 la sentenza della Corte di Giustizia dell'Unione europea che ha dichiarato l'invalidità del *Safe Harbour* (strumento legittimante il trasferimento dei dati negli USA) ha scosso gli equilibri internazionali determinando l'inizio di una fase di intensi colloqui tra Stati Uniti ed Europa per l'individuazione di uno strumento se non sostitutivo, quantomeno alternativo ad esso. L'Autorità Garante italiana, quale membro del *Working Party Article* 29, ha partecipato attivamente a tali negoziati che hanno condotto ad un nuovo accordo, noto come *Privacy Shield*, il cui testo, dopo essere stato definitivamente approvato dagli Stati Membri in data 8 luglio 2016, è stato formalmente adottato dalla Commissione europea il successivo 12 luglio.

Particolare rilievo ha assunto poi l'attività del Garante nell'ambito delle discussioni sul nuovo Regolamento (UE) 2016/679, recentemente entrato in vigore dopo un *iter* legislativo durato più di 4 anni. Nella relazione sono evidenziati, tra le altre cose, i principali elementi di novità della nuova disciplina europea sul trattamento dei dati che includono: il potenziamento dei contenuti obbligatori dell'informativa, l'introduzione del diritto all'oblio ed alla portabilità dei dati, il principio dell'*accountability*, l'introduzione della figura del *Data Protection Officer* e della disciplina sulla contitolarità del trattamento e della ripartizione di responsabilità fra contitolari, obbligo generalizzato di notificare eventuali violazioni di dati personali, introduzione del *Privacy Impact Assessment*.

In aggiunta a quanto sopra, uno degli aspetti del nuovo Regolamento europeo che sicuramente ha suscitato e susciterà l'attenzione dei titolari del trattamento è dato dall'introduzione di sanzioni amministrative molto più rigide rispetto a quelle previste dalla normativa fino ad oggi in vigore, suggerendo sin da ora che, a differenza di quanto avvenuto in passato, la conformità con la legislazione in materia di *privacy* diventerà di primaria importanza per le imprese.

Con riferimento, infine, alle attività programmate per il 2016, per il primo semestre l'Autorità ha preannunciato tra le aree di interesse della propria attività ispettiva, i trattamenti effettuati da società di carattere multinazionale che trasferiscono i dati, nell'ambito di flussi intra-gruppo, in paesi non appartenenti all'Unione europea avvalendosi delle garanzie contenute nelle *Binding Corporate Rules*; la corretta adozione delle misure minime di sicurezza da parte di soggetti pubblici e privati che effettuano trattamenti di dati sensibili, nonché i trattamenti effettuati da organismi sanitari in relazione all'istruzione del *dossier* sanitario.