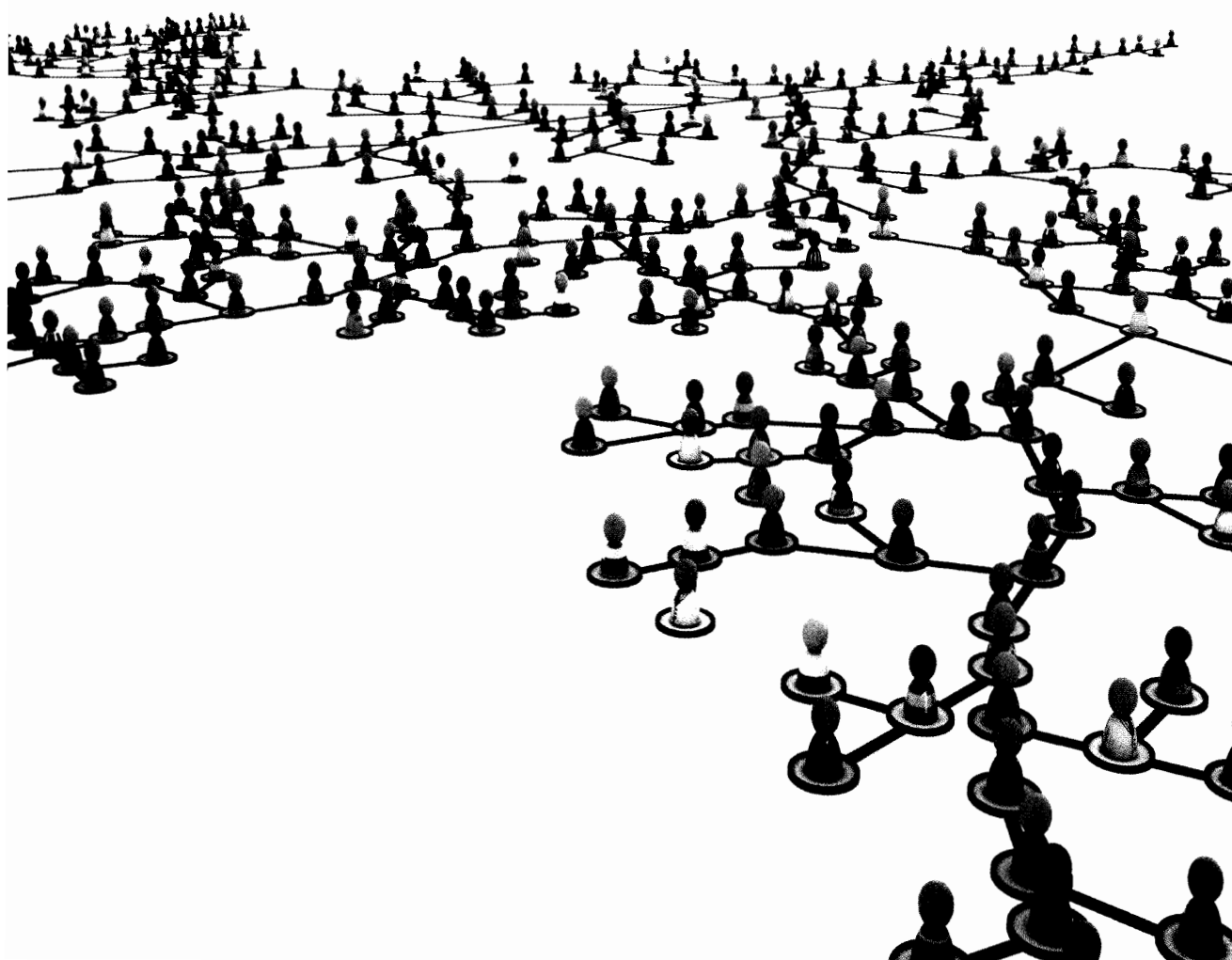


Stato di attuazione del Codice in materia di protezione dei dati personali



PAGINA BIANCA

I. Stato di attuazione del Codice in materia di protezione dei dati personali

1. PRINCIPALI INTERVENTI DELL'AUTORITÀ NEL 2010

1.1. PROVVEDIMENTI PIÙ SIGNIFICATIVI

1.1.1. Trattamenti collegati allo svolgimento di funzioni di giustizia

Nel periodo di riferimento l'applicazione della normativa sulla protezione dei dati personali all'esercizio di funzioni giurisdizionali è stata oggetto di decisioni di particolare delicatezza, in relazione alle implicazioni di carattere generale, riguardanti la tutela di diritti fondamentali della persona nel quadro costituzionale dei rapporti tra poteri.

In risposta ad alcune istanze che avevano lamentato l'illecito utilizzo in giudizio di dati sensibili e giudiziari, l'Autorità ha sottolineato che, ai sensi dell'art. 160 del Codice, spetta al giudice adito pronunciarsi, in base alle pertinenti disposizioni processuali, sulla validità, l'efficacia e l'utilizzabilità di atti presentati nell'ambito del procedimento giudiziario, anche se basati su un trattamento illecito di dati personali (*Provv.* 23 settembre 2010 [doc. *web* n. 1756065]; *Provv.* 4 novembre 2010 [doc. *web* n. 1770943]; *Provv.* 17 novembre 2010 [doc. *web* n. 1779765]).

Al termine di verifiche svolte in collaborazione con il Consiglio di Stato ed il TAR del Lazio, è emerso —pur in un quadro di complessivo rispetto delle regole— che gli uffici giudiziari amministrativi dovranno accrescere le misure di sicurezza a protezione dei dati giudiziari (*Provv.* 23 settembre 2010 [doc. *web* n. 1753845]). In particolare, il Garante ha fornito specifiche indicazioni sia per il trattamento dei dati svolto senza l'ausilio di strumenti elettronici —soprattutto per una maggiore protezione dei fascicoli processuali— sia per il trattamento con l'ausilio di strumenti elettronici, specie per le modalità di accesso dei magistrati e del personale amministrativo al Nuovo sistema informativo della giustizia amministrativa (NSIGA).

L'Autorità si è altresì occupata della diffusione dei provvedimenti giurisdizionali su supporti cartacei ed informatici nonché mediante reti di comunicazione elettronica, fonte preziosa per lo studio e l'accrescimento della cultura giuridica e strumento indispensabile di controllo da parte dei cittadini dell'esercizio del potere giurisdizionale. In taluni casi, tuttavia, riportare le generalità delle parti può risultare in contrasto con esigenze di tutela della loro dignità e riservatezza.

Al riguardo, sulla base di segnalazioni e quesiti ricevuti, dopo ampia consultazione con gli operatori del settore, sono state adottate specifiche linee-guida (*Prov. 2 dicembre 2010 [doc. web n. 1774813], in G.U. 4 gennaio 2011, n. 2*) —che non si applicano all'attività giornalistica, oggetto di altra disciplina— sulla pubblicazione di atti giurisdizionali per la finalità di informazione giuridica. In sostanza sono stati individuati i casi in cui chi intende pubblicare l'atto giudiziario deve oscurare i dati delle parti e gli elementi utili ad indentificarle (in particolare ove si tratti di minori e di procedimenti relativi a rapporti di famiglia), nonché i criteri per richiedere l'“anonimizzazione”; questa, che può essere anche decisa d'ufficio dal giudice, va annotata sull'atto, in modo che chi lo riceve provveda prima di diffonderne il contenuto.

1.1.2. Pubblicazione di atti sul web da parte di amministrazioni pubbliche

Le “*Linee-guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web*” (*Prov. 2 marzo 2011 [doc. web n. 1793203], in G.U. 19 marzo 2011, n. 64*), adottate dopo ampia consultazione, definiscono un quadro unitario delle misure che la p.a. deve adottare per la pubblicazione di atti e documenti sui propri siti *web* istituzionali.

In termini generali, le amministrazioni pubbliche possono mettere in rete atti o documenti contenenti dati personali solo sulla base di una previsione normativa, rispettando i principi di necessità, proporzionalità e pertinenza ed il generale divieto di diffondere dati sulla salute. Contro i rischi di cancellazioni e modifiche delle informazioni presenti *online* vanno adottate adeguate misure tecnologiche. La reperibilità dei documenti deve essere, se possibile, assicurata attraverso motori di ricerca interni al sito della singola amministra-

zione, allo scopo di garantire un accesso coerente con la finalità per la quale i dati sono stati resi pubblici, evitando il rischio di estrazione arbitraria dei dati, che ne renderebbe incontrollabile l'uso. Con riguardo alla conservazione *online* dei dati, in mancanza di specifiche disposizioni le pp.aa. devono individuare limiti temporali congrui alle finalità del trattamento, e provvedere successivamente a rimuoverli.

Ancora, contro i rischi di riproduzione e riutilizzo dei *file* contenenti dati personali, devono essere installati *software* e sistemi di *alert* che consentano di riconoscere e segnalare accessi anomali, al fine di mettere in atto contromisure adeguate.

1.1.3. Trattamenti di dati sensibili, in particolare relativi allo stato di salute

L'esame delle finalità per le quali è ammesso il trattamento e l'individuazione delle cautele da osservare sono stati i profili specifici oggetto di diversi provvedimenti adottati dall'Autorità in questa materia.

In un *parere* (17 novembre 2010 [doc. *web* n. 1769451]) reso alla Commissione per l'accesso ai documenti amministrativi presso la Presidenza del Consiglio dei ministri, aderendo a quanto prospettato dalla Commissione stessa, il Garante ha affermato che un genitore non può accedere presso la Asl alla documentazione sanitaria della figlia minore che, all'insaputa del padre, si sia rivolta ad un consultorio per farsi prescrivere farmaci contraccettivi. Va infatti riconosciuta alla minore una sfera di riservatezza che garantisca effettivamente la sua autodeterminazione, e permetta l'utilizzo delle strutture autorizzate, che possono assicurare le necessarie garanzie nell'erogazione delle prestazioni.

In relazione al servizio di consegna a domicilio, offerto da un supermercato agli acquirenti invalidi o disabili, il Garante ha deciso (*Prov. 13* maggio 2010 [doc. *web* n. 1729156]) che non può essere chiesta, a tal fine, copia del verbale di invalidità, essendo sufficiente che la persona, al momento della prima richiesta del servizio, esibisca un qualsiasi documento che attesti il suo stato. Il trattamento dei dati è quindi risultato sproporzionato rispetto alle finalità perseguite ed al punto vendita oggetto della segnalazione l'Autorità ha anche prescritto di distruggere le copie dei verbali medici già acquisite.

Oggetto di un altro *provvedimento* (19 gennaio 2011 [doc. *web* n. 1787877]) sono state

le modalità con cui fornire agli interessati l'informativa in relazione ad un progetto di sorveglianza epidemiologica dei tumori nella popolazione militare impegnata in Bosnia-Herzegovina e nel Kosovo. Il progetto prevede in particolare che il Ministero della difesa fornisca all'Istituto superiore di sanità i dati personali dei militari (da incrociare con quelli di altre banche dati), per valutare se la permanenza nei Balcani, ove è stato fatto uso di munizioni ad uranio impoverito, abbia avuto conseguenze sulla salute dei soldati.

Per l'ingente numero delle persone coinvolte è stata prevista, in luogo dell'informativa resa a ciascun interessato, la pubblicazione della medesima sui siti del Ministero della difesa, delle singole forze armate e delle associazioni del personale in quiescenza, oltre che su due quotidiani di larga diffusione nazionale. L'Autorità, per assicurarne la massima conoscibilità, ha prescritto la pubblicazione dell'informativa anche sul sito dell'Istituto superiore di sanità e la sua agevole visibilità sino alla conclusione del progetto (art. 154, comma 1, lett. *c*), del Codice e art. 6, comma 4, del codice di deontologia e buona condotta per i trattamenti di dati per scopi statistici e scientifici).

In relazione ad una ricerca sociologica svolta tra aderenti ad un istituto religioso, con un questionario relativo, tra l'altro, ad opinioni politiche, abitudini sessuali, condizioni di salute, sono state prescritte (art. 154, comma 1, lett. *c*) e *d*), del Codice) le misure idonee ad escludere il rischio di interconnessione tra i dati in parola, raccolti da una società esterna, ed i nominativi degli aderenti all'istituto che avevano preso parte all'iniziativa; in particolare, è stata vietata la trasmissione dei questionari agli altri soggetti coinvolti nella ricerca ed ordinata la distruzione dei medesimi al termine della ricerca stessa. Ciò per impedire l'identificazione, sia pur indiretta, degli interessati, in considerazione anche del loro ristretto numero (*Prov. 1° aprile 2010 [doc. web n. 1721183]*).

1.1.4. Giornalismo ed informazione online

Il delicato equilibrio tra libertà di informazione e riservatezza degli interessati è stato in diverse decisioni individuato applicando il principio dell'essenzialità dell'informazione (cfr. art. 137, comma 3, del Codice e art. 6 del codice di deontologia sul trattamento dei dati nell'attività giornalistica - Allegato A.1. al Codice).

Riconoscendo che rientra nel diritto alla manifestazione del pensiero la pubblicazione di atti giudiziari non più coperti da segreto, è stata prescritta la cancellazione dei dati non essenziali riportati in un'ordinanza di custodia cautelare — numeri di telefono, recapiti e codici fiscali di diverse persone ivi citate — ad un'associazione che, a corredo di una notizia, aveva diffuso *online* il testo del *provvedimento* giudiziario (v. art. 139, comma 5, del Codice; *Prov. 29 settembre 2010* [doc. *web* n. 1763096]).

In un altro caso è stata ritenuta di rilevante interesse pubblico la notizia, fornita dalla seguace di un'associazione in un'intervista pubblicata su un sito Internet, delle vessazioni da lei stessa subite e delle cause dei decessi di altri seguaci, talvolta con menzione delle relative patologie. L'Autorità ha però prescritto di citare le persone interessate — la cui riservatezza è meritevole di tutela anche dopo la morte — solo con nomi di fantasia, ovvero con le iniziali puntate, avendo ravvisato nella pubblicazione del loro cognome una violazione della sfera di riservatezza, del decoro e della dignità delle persone (cfr. art. 139, comma 5, del Codice; *Prov. 1° luglio 2010* [doc. *web* n. 1738303]).

L'ulteriore diffusione, anche sul *web*, dei dati personali relativi ad alcune adozioni è stata vietata ad un'emittente televisiva (*Prov. 6 maggio 2010* [doc. *web* n. 1718239]) in relazione ad alcune trasmissioni, nel corso delle quali erano stati forniti elementi che rendevano identificabili gli adottati, favorendone la ricerca da parte di genitori e fratelli naturali. L'Autorità ha ravvisato in tale condotta un contrasto con la *ratio* della disciplina in materia di adozioni, la quale individua specificamente i presupposti perché l'adottato possa accedere ad informazioni che riguardano la sua origine (v. artt. 27, 28, e 73, l. 4 maggio 1983, n. 184, modificata dalla l. 28 marzo 2001, n. 149) e, di conseguenza, con il Codice (v. artt. 2, 11, 137). Nei confronti dell'emittente è stato anche avviato un procedimento per applicare sanzioni pecuniarie, nonché la segnalazione all'autorità giudiziaria, poiché il blocco disposto in relazione ad una delle puntate non è stato osservato.

Nei confronti di un'altra emittente è stata vietata l'ulteriore diffusione della parte di una intervista in cui una donna, narrando gli abusi subiti in famiglia quando era minorenni, aveva fatto riferimento agli abusi subiti anche dalla sorella, minorenne al momento dell'intervista, con dati che ne consentivano l'identificazione (*Prov. 16 settembre 2010*

[doc. *web* n. 1753383]). Come più volte ribadito dal Garante (v. *Relazione* 2009, p. 7 ss.), l'obbligo del giornalista di tutelare la riservatezza dei minori, in particolare se vittime di abusi sessuali, prevale infatti sul diritto di cronaca. Ciò anche in relazione ad interviste a soggetti che liberamente rendano noti i dati relativi ai minori interessati (cfr. art. 114, comma 6, c.p.p.; art. 7 del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica; Carta di Treviso).

1.1.5. Comunicazioni elettroniche e acquisizioni su larga scala di immagini per la pubblicazione online

In relazione all'utilizzo massiccio di tecnologie applicate a dimensioni diverse della vita quotidiana, l'Autorità ha assunto decisioni per diversi profili innovative.

Il Garante ha bloccato (*Prov. 9 settembre 2010* [doc. *web* n. 1750529]) qualsiasi trattamento effettuato da *Google* sui frammenti di comunicazioni elettroniche captati sul territorio italiano, tramite appositi *software*, dalle *Google car* che, per il servizio *Street View*, acquisiscono immagini panoramiche a livello stradale. Diversamente da quanto prospettato dalla Società, l'Autorità ha ritenuto che il carattere sistematico della raccolta, protrattasi per circa due anni, rende concreta l'eventualità che le informazioni, pur frammentarie, abbiano natura di dati personali. Inoltre, gli atti sono stati trasmessi all'autorità giudiziaria per l'accertamento di eventuali violazioni delle norme penali che proteggono le comunicazioni effettuate con un sistema telematico (cfr. artt. 617-*quater* e *quinquies* c.p.).

Inoltre, sempre con riferimento al servizio *Street View*, a pena di rilevanti sanzioni pecuniarie è stato prescritto (*Prov. 15 ottobre 2010* [doc. *web* n. 1759972]) alla società californiana di fornire dettagliate informazioni sul passaggio delle *Google car*, sia sul proprio sito, sia sulle pagine di cronaca di almeno due quotidiani, sia su emittenti locali, anche per consentire agli interessati di allontanarsi dai luoghi in cui vengono riprese le immagini.

Al riguardo sono state applicate le norme del nostro ordinamento, con significativa innovazione rispetto ad alcuni casi precedenti, poiché il citato trattamento è per sua natura effettuato con strumenti situati sul territorio italiano (art. 5 del Codice), ed è stato