



Osservatorio sull'Analisi d'Impatto della Regolazione

CAROLINA RAIOLA

L'AIR nel Garante per la protezione dei dati personali

S 6/2012

gennaio 2012



L'AIR NEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Variazioni e integrazioni
rispetto alla scheda precedente (febbraio 2011)

Non si registrano novità relative all'attività di analisi d'impatto della regolazione del Garante per la protezione dei dati personali. La consultazione dei soggetti interessati ha trovato invece nuovo slancio con riferimento alla redazione di due documenti di 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 e in quella di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica (par. 4).

INDICE

1. L'UE, il Garante europeo per la protezione dei dati e gli altri Paesi	7
<i>Le istituzioni dell'UE</i>	7
<i>Il Garante europeo per la protezione dei dati</i>	7
<i>Le esperienze condotte negli altri Paesi</i>	8
2. Gli aspetti normativi.....	9
3. Il processo di introduzione di strumenti di <i>better regulation</i>	9
4. L'esperienza realizzata.....	10
5. Le prospettive.....	14

Questo documento è soggetto a licenza Creative Commons Attribuzione-Non commerciale-Non opere derivate 2.5.

Citare questo documento come: C. Raiola, L'AIR nel Garante per la protezione dei dati personali, Osservatorio sull'Analisi di Impatto della Regolazione, www.osservatorioair.it, gennaio 2012, S 6/2012.

1. L'UE, il Garante europeo per la protezione dei dati e gli altri Paesi

Le istituzioni dell'UE

Nella UE non esistono norme o documenti di indirizzo che, in via diretta, impongano ai garanti per la protezione dei dati di avviare procedure formali di analisi d'impatto della regolazione.

Un'indiretta attenzione ai costi e all'efficienza della normativa sulla privacy è stata però posta, nel 1995, dall'art. 7 lettera b della direttiva n. 95/46/CE. Infatti, la direttiva quadro comunitaria in materia di protezione dei dati personali sancisce, con la cosiddetta "clausola del bilanciamento degli interessi", il principio per cui la valutazione della legittimità di un trattamento dei dati esige la comparazione tra gli interessi di chi vuole utilizzare i dati e quelli del soggetto a cui i dati si riferiscono. Il rispetto di tale clausola troverebbe un'adeguata realizzazione proprio attraverso la valutazione dei costi e dei benefici e, dunque, attraverso l'analisi di impatto¹.

L'art. 29 della direttiva n. 95/46/CE ha poi istituito l'*Art. 29 Data Protection Working Party* (altrimenti detto *Gruppo articolo 29*), un gruppo di lavoro indipendente, e con compiti consultivi dell'Unione europea, al quale partecipa il Garante italiano della protezione dei dati personali insieme a tutte le altre autorità degli Stati membri con competenze in materia. Il *Gruppo* si occupa, tra l'altro, di verificare gli effetti sul diritto alla riservatezza della regolamentazione dell'Unione e dei Paesi membri.

Il Garante europeo per la protezione dei dati

L'analisi di impatto sulla privacy si è rafforzata nel tempo. I Garanti dei 50 paesi che hanno partecipato alla 31ma Conferenza internazionale delle autorità di protezione dei dati hanno approvato una risoluzione (cd. Risoluzione di Madrid) sugli standard che ciascun ordinamento giuridico dovrebbe assicurare in materia di privacy; tra questi compare il principio di potenziare le valutazioni preventive di impatto qualora si mettano in atto nuovi sistemi, metodi e tecnologie

¹ Il rapporto tra la clausola del bilanciamento degli interessi e l'analisi dei costi e dei benefici della regolazione in materia di privacy è preso dall'intervento di Marco Maglio "Analisi economica del diritto alla riservatezza" nella Conferenza Internazionale "Privacy: da costo a risorsa", tenuta a Roma, presso la sede dell'Autorità Garante, nel dicembre 2002. L'intervento è stato pubblicato nel volume "Da costo a risorsa. La tutela dei dati personali nelle attività produttive", a cura di Gaetano Rasi, Istituto Poligrafico e Zecca dello Stato, 2003.

che intervengano nel trattamento dei dati personali². La definizione di questo standard formalizza a livello internazionale un'attività già piuttosto praticata dall'Unione. L'attività di consulenza del Garante europeo per la protezione dei dati (GEPD) è, ad esempio, esercitata soprattutto in funzione dell'impatto che le proposte legislative elaborate dagli organismi europei nei vari settori hanno sul livello della protezione dei dati³. Il GEPD ha, infatti, il compito di sorvegliare e assicurare che le istituzioni e gli organismi europei rispettino le disposizioni UE in materia di protezione dei dati, anche fornendo pareri e osservazioni sulla normativa d'interesse. Tale funzione è considerata dallo stesso Garante europeo un'attività strategica, che consente di analizzare le implicazioni in materia di tutela dei dati personali e di discutere possibili alternative in una fase precoce del processo di drafting⁴.

Le esperienze condotte negli altri Paesi

Sempre relativamente all'attività di analisi dell'impatto sulla privacy, l'Information Commissioner's Office (l'ICO, il garante per la privacy inglese) ha pubblicato nel 2009 il *Privacy Impact Assessment (PIA) handbook*. Le linee guida ICO illustrano gli step dell'analisi d'impatto sulla privacy e sono indirizzate in prima battuta a tutte le organizzazioni destinatarie delle norme che sviluppano singoli progetti in grado di esercitare implicazioni sulla riservatezza dei cittadini. Il Garante inglese ha però concepito l'*Handbook* come un framework utile anche per gli organismi che hanno funzione di regolazione e ha specificato che, in ogni caso, al fine di prevenire conseguenze inaspettate sul diritto alla riservatezza, l'analisi deve avere carattere preventivo⁵.

2 Cfr. Risoluzione di Madrid – Conferenza internazionale delle autorità di protezione dati e privacy. Standard internazionali in materia di protezione dei dati personali e privacy, art. 22, lettera f, 5 novembre 2009.

3 Cfr. le Relazioni annuali del Garante europeo per la protezione dei dati. Si veda, sull'analisi d'impatto sulla privacy, anche il Policy Paper del GEDP *Monitoring and ensuring compliance with regulation (EC)*, Brussels, 13 dicembre 2010.

4 Per le funzioni del GEPD, si veda il Regolamento (CE) n. 45/2001, artt. 41, 46, 47. Riguardo all'attività di consulenza, cfr. Garante europeo per la protezione dei dati, Relazione annuale 2009, Unione europea 2011, pp. 50 e seguenti e p. 93.

5 Cfr. Information Commissioner's Office, *Privacy Impact Assessment (PIA) handbook*, 2009.

2. Gli aspetti normativi

L'obbligo per il Garante di condurre l'analisi di impatto dei propri provvedimenti si evince in via interpretativa dall'articolo 12 della legge 229/2003, che impone alle autorità amministrative indipendenti con funzioni di controllo, vigilanza o regolatorie di dotarsi di forme o metodi di AIR.

3. Il processo di introduzione di strumenti di *better regulation*

L'analisi di impatto della regolazione non è ancora stata introdotta in modo formale dal Garante della protezione dei dati personali: nessun regolamento concernente l'AIR è stato approvato, nessuna fase di sperimentazione è stata ufficialmente avviata e non esiste un Dipartimento o un Servizio con il compito di analizzare l'efficacia dei provvedimenti formulati. All'opposto, il Garante verifica sistematicamente, nel corso della propria consueta attività ispettiva⁶, l'impatto che i provvedimenti adottati dagli altri organismi (o dagli operatori che utilizzano i dati personali) hanno sul diritto alla protezione dei dati.

Il Garante assicura indirettamente efficienza al proprio processo decisionale soprattutto attraverso forme di consultazione, che consentono agli interessati di partecipare in via diretta alla formulazione delle *policies* e che costituiscono un passaggio chiave e indispensabile per l'introduzione dell'analisi di impatto della regolamentazione⁷. Con la consultazione si rende infatti possibile l'individuazione di molte esigenze (di tipo giuridico, economico e sociale) da cui l'AIR parte: si perfezionano lo studio del contesto da regolamentare, la rilevazione delle esigenze dei destinatari e, all'occorrenza, anche l'elaborazione delle opzioni alternative di intervento. Nella formulazione dei propri provvedimenti, il Garante assicura agli *stakeholders* la possibilità di intervenire nei procedimenti di adozione degli atti svolgendo sia incontri informali e formali, sia consultazioni pubbliche telematiche. La consultazione degli *stakeholders* più influenti e degli esperti è in genere funzionale sia al reperimento di informazioni sul contesto da regolare, sia ad una stesura concordata delle prime bozze di provvedimento; la consultazione pubblica dei destinatari dell'intervento, invece, pur promossa

6 Cfr. Relazione Annuale 2007, p. 151. Anche nelle successive relazioni annuali tale attività ispettiva è ribadita dal Garante, che ne specifica dettagli e programmazione (cfr. Relazione Annuale 2009, p. 239).

7 Cfr. Dipartimento della funzione pubblica (2001), *La consultazione nell'analisi dell'impatto della regolazione*, Rubbettino, 2001, p. 11.

talvolta a sostegno delle fasi istruttorie, contribuisce soprattutto a migliorare l'efficienza della bozza finale del documento. Nel caso della sottoscrizione di Codici deontologici e di buona condotta, è espressamente previsto dal Garante che il processo di formulazione del provvedimento sia organizzato in modo da incoraggiare “la proficua cooperazione tra i soggetti appartenenti alle categorie interessate e la collaborazione dei soggetti interessati nell'organizzazione e nello svolgimento dei lavori di redazione del codice, fornendo, salva diversa loro scelta, un supporto anche logistico e tecnico o da parte di esperti, nonché nell'utilizzo di strumenti elettronici, anche per agevolare lo scambio delle informazioni e il confronto e la condivisione delle proposte e dei contributi fra i partecipanti”⁸. Relativamente alla natura delle disposizioni oggetto di pubblica consultazione, l'approvazione nel 2006 del Regolamento sulla procedura per la sottoscrizione dei codici deontologici e di buona condotta⁹ ha avuto probabilmente l'effetto di garantire la partecipazione procedimentale soprattutto su schemi di linee guida del Garante¹⁰.

E' però interessante segnalare che l'8 gennaio del 2008 sono stati banditi concorsi pubblici finalizzati (tra l'altro) al reclutamento di un dirigente con documentata esperienza in materia di analisi di impatto della regolamentazione¹¹, al fine di incrementare l'esiguo organico di cui l'Autorità ha potuto fino a quella data disporre¹² per l'avvio e l'adozione di tecniche di AIR. Le attività di analisi d'impatto, nonostante le procedure di selezione siano andate a buon fine, non sono tuttavia ancora partite per motivi di organizzazione interna e carenza di personale nelle diverse direzioni dell'Autorità.

4. L'esperienza realizzata

Pur non conducendo attualmente un'analisi di impatto formalizzata e strutturata sulla propria regolamentazione, il Garante per la Privacy mostra una certa sensibilità per la valutazione degli

8 Art. 4, c. 2 del Regolamento n. 2 del 2006.

9 Si veda la nota n. 8, *infra*.

10 Si veda il paragrafo n. 4, *infra*.

11 I relativi bandi sono stati pubblicati nella Gazzetta Ufficiale – quarta serie speciale – 8 gennaio 2008, n.2. (www.garanteprivacy.it/garante/doc.jsp?ID=1477556)

12 Cit. Relazione annuale 2008, p. 288.

effetti sociali ed economici dei provvedimenti più rilevanti che adotta. Oltre agli interventi di consultazione formale e informale prima elencati, il Garante ha ad esempio affrontato nel dicembre del 2002 (in occasione dell'imminente promulgazione del Codice della privacy che poi sarebbe stato adottato con il decreto legislativo 30 giugno 2003 n. 196) il tema del costo della regolamentazione inerente alla protezione dei dati personali. Questa occasione di riflessione *a priori* non ha prodotto alcuna analisi formale sull'impatto economico del Codice sulle imprese o sulle organizzazioni, ma ha costituito l'occasione per il Garante di effettuare uno studio sugli effetti benefici derivanti dall'emanazione del Codice e di riflettere sia sul principio del bilanciamento degli interessi (si veda il paragrafo 1), sia sullo snellimento degli adempimenti a carico delle aziende¹³.

Ai sensi dell'art. 24, comma 1, lett. g), del Codice Privacy, il Garante ha, ad esempio, dato attuazione al principio di bilanciamento degli interessi per il provvedimento relativo alle comunicazioni, tra intermediari finanziari appartenenti ad un medesimo gruppo, di dati personali relativi alle segnalazioni di operazioni considerate sospette ai sensi della normativa antiriciclaggio. L'attività di richiesta di trattamento dei dati degli interessati per questo tipo di comunicazioni è stato ritenuto dalle banche come un'incombente "estremamente gravosa, oltre che sproporzionata, valutata nel giudizio dell'equo temperamento degli interessi coinvolti". Il Garante, considerando come "di portata generale" un quesito proveniente dalle banche, ha dunque tenuto conto degli oneri legati all'attività di trattamento dei dati e formulato di conseguenza il proprio provvedimento, ammettendo come lecita la comunicazione infragruppo nella fattispecie considerata¹⁴. Quindi, sebbene alcune forme di bilanciamento degli interessi trovino un certo spazio nell'attività regolatoria del Garante, nessuna analisi di impatto della regolazione in senso proprio è stata fino ad ora avviata, sperimentata o realizzata.

Sporadiche forme di valutazione *ex post* della propria attività regolatoria sono svolte dal Garante attraverso l'esame di osservazioni e quesiti provenienti dai destinatari della disciplina di protezione dei dati personali. Un esempio di tali valutazioni è il citato provvedimento sulle comunicazioni tra intermediari finanziari appartenenti ad un medesimo gruppo; un altro è la pubblicazione della Guida pratica e misure di semplificazione per le piccole e medie imprese. La stesura della Guida ha fatto

13 Cit. scheda informativa sul Codice della Privacy, disponibile sul sito web del Garante all'url www.garanteprivacy.it/garante/doc.jsp?ID=1028065.

14 Si veda il provvedimento *Misure relative alle comunicazioni fra intermediari finanziari appartenenti al medesimo gruppo in materia di antiriciclaggio* - 10 settembre 2009, pubblicato nella G.U. n. 267 del 16 novembre 2009.

seguito alla manifestata esigenza, da parte delle associazioni di categoria, di poter far riferimento a un documento che delineasse con chiarezza orientamenti e linee di comportamento conformi al Codice in materia di protezione dei dati personali¹⁵.

Il Garante per la protezione dei dati personali ha in ogni caso maturato esperienza nella *better regulation* soprattutto attraverso forme di consultazione (sia dei principali *stakeholders*, sia del grande pubblico) a sostegno della propria attività di regolazione, avviando (fino ad oggi) otto consultazioni pubbliche telematiche dirette in via preferenziale ai segmenti destinatari dei provvedimenti in esame, con finalità sia esplorative (per le tre consultazioni dal 2004 al 2006), sia di commento a schemi di provvedimenti (per le cinque consultazioni successive).

La prima consultazione svolta dal Garante (aperta dal 31 dicembre 2004 al 15 gennaio 2005) ha avuto una funzione di ricognizione e ha completato l'istruttoria preliminare su quattro temi su cui l'Autorità era in procinto di adottare provvedimenti: carte di fedeltà; televisione satellitare e interattiva; etichette intelligenti; videotelefonini. I destinatari di queste misure (associazioni di utenti e di consumatori; operatori nei settori interessati; singoli cittadini) sono stati chiamati a far pervenire, nel quadro della consultazione, osservazioni, informazioni e commenti utili in merito ai quattro temi. La stessa finalità è stata perseguita per le due consultazioni pubbliche successive: quella sul trattamento dei dati personali relativi all'affidabilità e puntualità dei pagamenti nel settore della telefonia, aperta dal 1° maggio 2005 al 20 giugno 2005, è stata avviata per raccogliere elementi di valutazione e osservazioni utili al Garante in vista dell'adozione del codice di deontologia per il settore della telefonia (previsto dall'art. 117 del d. lg. 196/2003); quella sulla riservatezza dei dati nell'ambito della gestione dei condomini (8 febbraio 2006 – 27 febbraio 2006) è stata aperta allo scopo di definire un provvedimento in materia che tenesse conto delle principali problematiche emergenti dalla prassi.

Le tre consultazioni pubbliche telematiche appena citate hanno consentito al Garante di approfondire le questioni concernenti la materia da regolare prima di adottare le proprie decisioni; le cinque successive, svolte dal settembre 2007 al marzo 2011, sono state invece promosse allo scopo di acquisire riscontri sull'adeguatezza di provvedimenti già definiti. Se le prime ponevano quindi questioni aperte sulle caratteristiche dell'ambito da regolare, le seconde hanno adottato la forma del *notice and comment* (pubblicazione della bozza del provvedimento allo scopo di ottenere commenti

15 Si veda la delibera del Garante n. 21 del 24 maggio 2007.

su di essa) e (come espressamente è riportato in taluni casi)¹⁶ sono state precedute da forme di consultazione non telematiche, chiuse al grande pubblico e aperte solo ai principali *stakeholders*. La prima delle cinque consultazioni di tipo *notice and comment* svolte dal Garante ha interessato misure in tema di conservazione di dati di traffico telefonico per finalità di accertamento e repressione dei reati (consultazione aperta dal 19 settembre 2007 al 31 ottobre 2007); le consultazioni pubbliche successive hanno garantito la partecipazione dei soggetti interessati alla stesura di quattro linee guida relative alla tutela dei dati personali nel settore della sanità e nelle pubblicazioni sul web. Per il settore sanitario, le linee guida hanno indirizzato il trattamento dei dati personali effettuati per promuovere studi clinici e sperimentare medicinali (consultazione pubblica aperta dal 29 novembre 2007 al 15 febbraio 2008); il fascicolo sanitario elettronico e il dossier sanitario (5 marzo 2009 – 31 maggio 2009); i referti on-line (avviata il 15 luglio 2009 e chiusa il 30 settembre 2009). In ordine di tempo, l'ultima consultazione pubblica condotta dal Garante è quella relativa alla stesura di 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. Lo schema di provvedimento¹⁷ è stato pubblicato sul sito istituzionale del Garante e sul sito del Governo; la consultazione è rimasta aperta per 45 giorni, dal 15 dicembre 2010 al 31 gennaio 2011; a seguito della ricezione delle osservazioni è stata poi pubblicata la versione definitiva delle linee guida, il 2 marzo 2011.

Altre forme di consultazione degli *stakeholders* si affiancano all'attività di consultazione pubblica: tavoli e incontri sono organizzati ai fini della stesura di provvedimenti di carattere generale per raccogliere dati e informazioni e per definire di stime di vantaggi e svantaggi associati all'introduzione dell'atto regolatorio nell'ordinamento. Un esempio è costituito dal caso delle Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di

16 Si veda ad esempio il sistema di consultazione che ha accompagnato la stesura delle Linee guida in tema di Fascicolo sanitario elettronico (doc. web n. 1598313, pubblicato sul sito del Garante per la protezione dei dati personali). Dopo aver svolto approfondimenti istruttori sulle iniziative di trattamento dei dati personali attraverso il Fascicolo sanitario elettronico promosse da organismi sanitari pubblici e privati, il Garante ha adottato il 22 gennaio 2009 un provvedimento recante le Linee guida, che è stato sottoposto alla consultazione di un gruppo di lavoro costituito presso il Ministero del lavoro, della salute e delle politiche sociali. Dopo questa consultazione chiusa, il 5 marzo del 2009 è stata avviata la consultazione pubblica dei soggetti e delle categorie interessate, al fine di acquisire gli ultimi riscontri prima della prescrizione delle misure indicate nelle Linee Guida.

17 Schema di Linee guida in materia di trattamento di dati personali effettuato da soggetti pubblici per finalità di pubblicazione e di diffusione sul web di atti e documenti adottati dalle pubbliche amministrazioni - 15 dicembre 2010.

informazione giuridica (delibera 2 dicembre 2010), per la cui stesura il Garante è ricorso a una consultazione in forma di audizione chiusa agli operatori di settore e agli editori¹⁸.

La disamina delle istanze (segnalazioni, reclami e quesiti) pervenute da soggetti interessati quali singoli cittadini, imprese o associazioni costituisce un ulteriore metodo di ascolto utile a monitorare gli interventi già posti in essere o a individuare vuoti nella regolazione¹⁹.

5. Le prospettive

Nel Garante per la protezione dei dati personali l'analisi degli effetti della regolazione in forma preventiva non è né sistematica né formalizzata, e la valutazione *ex post* è compiuta sporadicamente attraverso lo svolgimento dell'attività di gestione dei reclami legati ai provvedimenti emanati. Le consultazioni pubbliche on line e quelle formali e informali attraverso la tecnica dei gruppi di lavoro sono svolte dal Garante soprattutto allo scopo dichiarato di acquisire informazioni e stimolare l'intervento degli interessati nel processo decisionale, ma non appartengono ad alcuna procedura formale di analisi di impatto; è indubbio però che rappresentino un buono strumento di *better regulation* da cui partire per l'avvio di una sperimentazione dell'AIR. L'influenza del contesto internazionale, in cui sta crescendo l'attenzione per l'analisi dell'impatto, potrebbe costituire per il Garante un'ulteriore spinta per compiere ulteriori passi sulla strada del miglioramento della qualità della regolazione.

18 Si vedano i *vista* della delibera del 2 dicembre 2010.

19 I casi in cui l'adozione di provvedimenti è motivata con l'esame delle istanze sono individuabili sempre nella stesura delle linee guida. Si vedano, ad esempio, i casi delle linee-guida per il trattamento di dati dei dipendenti privati (23 novembre 2006); Linee guida del Garante per posta elettronica e internet (1° marzo 2007); linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali (19 aprile 2007); Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati (23 novembre 2006).