

## **Protezione dei dati, trasparenza e tecnologie della comunicazione**

PAGINA BIANCA

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

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

## 1. SINTESI DI ALCUNI PROVVEDIMENTI E ATTIVITÀ ISTITUZIONALI DI PARTICOLARE RILIEVO

Da uno sguardo d'insieme ai provvedimenti più significativi del periodo al quale questa Relazione si riferisce, di seguito sommariamente illustrati, emerge la varietà degli ambiti nei quali si sono posti problemi di protezione dati.

La complessità delle decisioni adottate ha riguardato tanto profili specificatamente giuridici, anche in relazione alla evoluzione del contesto normativo ed alle novità intervenute in materia di protezione dati, quanto tecnico-informatici.

### 1.1. GIUSTIZIA E PUBBLICA SICUREZZA

In materia di giustizia e ordine pubblico alcune deliberazioni collegiali si segnalano per il loro rilievo generale.

Su richiesta del Ministero della giustizia, il Garante ha espresso parere favorevole sullo schema di decreto dirigenziale riguardante la consultazione diretta, per via telematica, del Sistema informativo del Casellario (SiC) da parte delle amministrazioni pubbliche, dei gestori di pubblici servizi e dell'autorità giudiziaria (ai sensi dell'art. 39 d.P.R. 14 novembre 2002, n. 313, t.u. delle disposizioni in materia di Casellario giudiziario).

Il testo esaminato è volto, in particolare, ad assicurare un accesso selettivo ai soli dati giudiziari indispensabili per lo svolgimento degli accertamenti di competenza, tramite l'introduzione dell'apposito "certificato selettivo", per evitare che al soggetto richiedente siano rese disponibili, temporaneamente, anche eventuali iscrizioni di provvedimenti giudiziari non strettamente correlati agli accertamenti in corso (prov. 11 ottobre 2012 [doc. web n. 2091248]).

Permesso di  
soggiorno  
elettronico

Di significativa rilevanza anche il parere favorevole allo schema di decreto interministeriale che adegua il permesso di soggiorno rilasciato a cittadini di Paesi terzi al modello uniforme adottato dagli altri Stati comunitari. In base al nuovo decreto chi ottiene il permesso sarà fornito di una tessera, dotata di un microprocessore -contenente sia le informazioni necessarie a verificare l'autenticità del documento, sia i dati identificativi, la fotografia e le impronte digitali del titolare- che potrà essere letto esclusivamente dagli organi di controllo. I dati del cittadino straniero saranno registrati in un archivio elettronico presso il Centro elettronico nazionale (Cen) della polizia di Stato, conservati per i periodi puntualmente indicati nel decreto e potranno essere utilizzati solo per finalità relative alla verifica e alla gestione del permesso di soggiorno.

Nell'esprimere il parere l'Autorità si è riservata di valutare le regole tecniche con le quali saranno precisate le misure da adottare per garantire la riservatezza, l'integrità e la sicurezza dei dati trattati (provv. 5 giugno 2012 [doc. web n. 1908393]).

Il Garante ha altresì formulato il suo parere ai sensi dell'art. 54 del Codice, su due convenzioni relative all'accesso delle forze di polizia, tramite il Ced -Ministero dell'interno, a grandi banche dati.

Il parere sulla  
Convenzione tra il  
Ministero  
dell'interno e  
l'Inps

Il primo parere ha riguardato l'accesso alla banca dati dell'Inps, per l'adozione di misure di prevenzione e lo svolgimento di indagini sul tenore di vita e le disponibilità finanziarie degli indiziati di appartenere alla criminalità organizzata (l. 31 maggio 1965, n. 575) (provv. 2 febbraio 2012 [doc. web n. 1875293]).

La Convenzione in parola definisce in particolare la tipologia dei dati oggetto dell'accesso (dati anagrafici, retributivi, contributivi e pensionistici dei soggetti censiti dall'Inps), le finalità dell'accesso (esclusivamente quelle connesse allo svolgimento delle attività previste dalla suddetta normativa) ed il personale ad esso abilitato (operatori delle forze di polizia con qualifica di ufficiale o agente di polizia giudiziaria).

Al Ced è esplicitamente vietato duplicare le informazioni per creare banche dati autonome, nonché utilizzare dispositivi automatici che consentono la consultazione in forma massiva dei dati personali. Per quanto concerne la sicurezza, è previsto l'utilizzo del protocollo "ssl" per garantire le funzionalità di crittografia nel flusso dei dati. Inoltre, il Ced monitora gli accessi alla banca dati e rileva eventuali anomalie.

L'Autorità ha subordinato il proprio parere favorevole in particolare, all'indicazione che l'Allegato B della Convenzione, contenente l'analitica indicazione dei dati consultabili, costituisce parte integrante della medesima (parere 2 febbraio 2012 [doc. web n.1875293]).

Il secondo parere ha riguardato l'accesso ai dati e alle informazioni contenuti nel Sistema informatizzato di prevenzione amministrativa delle frodi sulle carte di pagamento (Sipaf) gestito dal Ministero dell'economia e delle finanze (l. 17 agosto 2005, n. 166 e d.m. del Ministero dell'economia e delle finanze 30 aprile 2007, n. 112) (prov. 12 luglio 2012 [doc. web n. 1915461]).

Anche in questo caso il testo della Convenzione individua principalmente le tipologie di dati e di informazioni oggetto dell'accesso e delimita le finalità (solo la prevenzione e repressione dei reati connessi all'utilizzo di carte di credito o di altri mezzi di pagamento).

I profili di sicurezza sono disciplinati in termini simili a quelli del precedente parere. In particolare il Ced deve impartire al personale abilitato direttive sulle responsabilità connesse all'accesso improprio alla banca dati ed all'uso illegittimo delle informazioni, non può duplicare le informazioni acquisite, né utilizzare dispositivi automatici per la consultazione dei dati in forma massiva; per quanto concerne la sicurezza, è previsto, tra l'altro, l'utilizzo del protocollo "ssl" per garantire le funzionalità di crittografia nel flusso dei dati.

Il Garante ha espresso parere favorevole sulla Convenzione valutando il suo contenuto conforme alla disciplina in materia di protezione di dati.

Di carattere individuale, invece, la decisione relativa alla segnalazione di un cittadino, debitore delle spese di giudizio per un contenzioso civile con una pubblica amministrazione, convocato da un commissariato di polizia per fornire notizie sulla sua situazione economica, in vista di un'eventuale procedura esecutiva a suo carico.

Al riguardo, il Garante ha osservato che l'acquisizione di tali notizie non rientra tra i compiti istituzionali della polizia di Stato e quindi viola le norme del Codice, che ammettono il trattamento e la comunicazione di dati da parte di soggetti pubblici sul fondamento di adeguata normativa o, in mancanza, per lo svolgimento delle funzioni istituzionali (artt. 18, comma 2 e 19, comma 2).

Il trattamento è stato pertanto dichiarato illecito con divieto di ogni ulteriore operazione da

Il parere sulla  
Convenzione tra il  
Ministero  
dell'interno e il  
Ministero  
dell'economia e  
delle finanze

Accertamenti di un  
commissariato  
sulla situazione  
debitoria di un  
cittadino

parte del commissariato e dell'ente pubblico creditore, salva la valutazione della sussistenza dei presupposti per la contestazione di violazioni amministrative (prov. 4 ottobre 2012).

## 1.2. ATTIVITÀ FISCALE E TRIBUTARIA

L'Autorità ha altresì adottato alcuni pareri relativi ad atti dell'amministrazione finanziaria volti al contrasto dell'evasione fiscale, caratterizzati da un complesso intreccio tra profili amministrativi e tecnici.

Agenzia delle  
entrate - Anagrafe  
tributaria

In particolare il Garante si è espresso sullo schema di provvedimento del Direttore dell'Agenzia delle entrate riguardante le modalità con le quali le banche dovranno comunicare all'Agenzia le informazioni relative ai conti correnti bancari (saldo iniziale e finale, importi totali degli accreditati e degli addebiti delle numerose tipologie di operazioni effettuate) (parere 17 aprile 2012 [doc. web n. 1886775]).

Tali dati dovranno poi essere ordinati su scala nazionale, a mezzo di procedure centralizzate, per la formazione di specifiche liste dei contribuenti a maggior rischio di evasione, secondo i criteri successivamente individuati dall'Agenzia.

Il Garante ha anzitutto evidenziato che la normativa pone rilevanti problemi, sia con riferimento all'eccezionale concentrazione presso l'Anagrafe tributaria di un'enorme quantità di informazioni personali, sia in relazione alle finalità di classificazione degli interessati, cui la raccolta di tali informazioni risulta preordinata. Ha al riguardo ribadito quanto rappresentato in sede di audizione presso la Commissione parlamentare di vigilanza sull'Anagrafe tributaria, sottolineando che non è in discussione l'esigenza di disporre delle informazioni necessarie per contrastare l'evasione fiscale, bensì l'integrale duplicazione presso l'Anagrafe stessa di una moltitudine di dati, che genera un incremento esponenziale dei rischi. Ha pertanto prescritto, per la trasmissione e la conservazione dei dati, misure di sicurezza di natura organizzativa e tecnica particolarmente rigorose.

Partecipazione dei  
comuni alla lotta  
all'evasione

In pari data l'Autorità ha dato parere favorevole ad un schema di provvedimento del Direttore dell'Agenzia delle entrate riguardante le modalità di partecipazione all'accertamento fiscale e contributivo da parte dei comuni, in attuazione della normativa di settore (v. da ultimo art. 18 del d.l. n. 78 del 31 maggio 2010, convertito dalla l. 30 luglio 2010, n. 122).

Il Garante ha espresso parere favorevole a condizione che -per tutti i soggetti coinvolti nel trattamento- siano garantiti *standard* di sicurezza minimi non inferiori a quelli già garantiti dall'Agenzia delle entrate in conformità al provvedimento del 18 settembre 2008 [doc. web n. 1549548].

In particolare ha stabilito che i comuni devono designare responsabili del trattamento i soggetti esterni dei quali decidano di avvalersi, fornendo loro adeguate istruzioni e vigilando sul trattamento tramite verifiche periodiche, anche a campione. Qualora tali soggetti siano designati responsabili da più comuni, non deve essere consentita la correlazione tra informazioni di competenza di comuni diversi (prov. 17 aprile 2012 [doc. web n. 1886825]).

Nell'ottobre 2012, l'Agenzia delle entrate ha trasmesso un nuovo schema di provvedimento, volto a regolare le modalità della comunicazione integrativa annuale all'archivio dei rapporti finanziari, sulla base delle osservazioni formulate dall'Autorità nel menzionato parere del 17 aprile 2012 [doc. web n. 1886775].

In particolare lo schema disciplina una nuova infrastruttura per la trasmissione dei dati, il "sistema di interscambio" che consente di automatizzare la raccolta dei dati presso gli operatori finanziari, riducendo i passaggi manuali che aumentano, di per sé, le possibilità di accessi non autorizzati.

Tuttavia, poiché l'architettura del sistema non è in grado di escludere interventi umani e prevede la possibilità di passaggi intermedi il Garante, nell'esprimere parere favorevole, ha in particolare chiesto all'Agenzia di adottare alcune misure di sicurezza, prevedendo anzitutto che il protocollo utilizzato per l'intercambio dei dati sia cifrato. L'Autorità ha inoltre individuato le misure da adottare per minimizzare i rischi di accessi abusivi e trattamenti non consentiti, tenendo conto delle esigenze dei piccoli operatori. Trascorso il termine previsto per la loro conservazione, i dati verranno automaticamente cancellati.

Il Garante ha in ogni caso previsto la procedura di verifica preliminare per ogni ulteriore utilizzo dei dati per altre finalità (ad es., controlli Isee) (parere 15 novembre 2012 [doc. web n. 2099774]).

Anagrafe tributaria  
- trasmissione e  
conservazione dei  
dati da parte di  
banche e operatori  
finanziari