MISURAZIONE ONERI AMMINISTRATIVI - MOA

PIANO DI MISURAZIONE DEGLI ONERI AMMINISTRATIVI DELLE IMPRESE

Scheda MOA **01.07**

Privacy
Piccole Medie Imprese (PMI)

(Ver. Def. 18.04.07)

Roma, Marzo 2007

INDICE

PREMESSA

Il Governo italiano ha deciso di imprimere alla politica di semplificazione un cambio di orientamento, in linea con le migliori pratiche emerse in ambito internazionale e con gli indirizzi più recenti definiti in sede europea (conclusioni del Consiglio Europeo dell'8 e 9 marzo 2007 in materia di Migliore Regolazione e "Programma d'azione per la riduzione degli oneri amministrativi nell'Unione europea", predisposto dalla Commissione a gennaio 2007). Gli interventi di semplificazione vanno, in particolare, mirati a una significativa riduzione degli "oneri amministrativi" che gravano sulle imprese e sui cittadini, nonché al contenimento dei costi dell'Amministrazione, anche attraverso un più efficiente impiego delle risorse umane e strumentali disponibili.

La Misurazione degli Oneri Amministrativi ed il PAS 2007

La misurazione degli oneri amministrativi in alcune aree prioritarie della normativa che disciplina l'attività di impresa è, quindi, una delle principali azioni sulle quali si concentra la strategia italiana, così come prevede il Piano Annuale di Semplificazione per il 2007. In questo contesto, è stata prevista una prima attività di misurazione degli oneri amministrativi che gravano sulle imprese derivanti dalla normativa sulla privacy, da svolgere in chiave sperimentale e dimostrativa nel primo trimestre 2007,, per disporre di un primo caso di misurazione finalizzato alla definizione operativa di interventi di semplificazione.

La metodologia

La metodologia di misurazione utilizzata è quella dello *EU Standard Cost Model*, il metodo adottato dalla Commissione europea sulla base delle esperienze condotte in alcuni Paesi europei di applicazione dello *Standard Cost Model*. Tale metodo prevede la misurazione di un sottoinsieme di costi, i c.d. "oneri amministrativi", stimando il costo di singoli obblighi informativi ("*Information Obligations*") imposti da norme di regolazione, per lo più attraverso interviste a un limitato numero di imprese rappresentative di una determinata categoria/settore di riferimento. Tali obblighi informativi consistono in tutti quegli obblighi che riguardano la raccolta, il mantenimento e la trasmissione di informazione a terzi e/o alle autorità pubbliche. E' importante considerare che, sulla base della metodologia SCM, la misurazione si concentra sugli oneri amministrativi che rappresentano un sotto-insieme, in molte occasioni molto rilevante, dei costi amministrativi. La misurazione infatti è mirata a stimare quei costi che l'impresa non sosterrebbe se non vi fosse una specifica disposizione di legge, ed è incentrata su un concetto di "onere amministrativo", per il quale la regolazione causa un anomalo fastidio e una distrazione non giustificabile dalle normali attività di impresa [1].

Vale sottolineare che lo *Standard Cost Model* è comunemente utilizzato a livello europeo quale strumento operativo per la misurazione e il calcolo degli oneri amministrativi, con una forte base pragmatica, In conseguenza di ciò, le stime effettuate sono ragionevolmente significative anche se statisticamente non

---

[1] Secondo lo "*Action programme for Reducing Administrative Burden in the EU*" della Commissione europea, "*unnecessary and disproportionate* ***administrative burdens*** *can have a real economic impact. They are also seen as an irritant and a distraction for business*".

rappresentative in senso tecnico e ciò in ragione del fatto che le tecniche di indagine SCM (così come adottate anche negli altri Paesi Europei), prevedono di intervistare un numero molto limitato di imprese che formano un campione *ragionato*. Inoltre, va ricordato che la metodologia SCM si riferisce ai soli oneri e cioè ai soli svantaggi/costi informativi e non anche ai vantaggi/benefici complessivi, riconducibili alla regolazione in esame. Infatti, la misurazione è volta a capire quali oneri amministrativi risultano essere eccessivi rispetto alle finalità della normativa stessa e ad individuare, su questa base, proposte di semplificazione.

Le PMI e la privacy

Per quanto concerne poi il caso specifico di misurazione, vale ricordare come gli oneri amministrativi legati alla *Privacy* costituiscano da tempo un'area sensibile per le imprese (si consideri ad esempio il Protocollo d'intesa tra Dipartimento della Funzione Pubblica e Confindustria, marzo 2006). E' in ragione di ciò che il PAS 2007 ha previsto la prima misurazione, a carattere dimostrativo, su questo specifico ambito di regolazione (ancorché la normativa in esame sia da considerare "comunitaria" e quindi costituisca parte dell'azione di misurazione all'interno dello specifico programma di misurazione della Commissione [2]). L'attività di misurazione degli oneri amministrativi descritta in questa scheda è stata pertanto condotta in tempi brevi (la raccolta dei dati è avvenuta nella settimana tra il 12 ed il 16 marzo 2007), in un ambito di regolazione giudicato particolarmente rilevante, ai fini della semplificazione delle imprese.

Il provvedimento in esame

Il provvedimento al quale si riferisce la misurazione è il Decreto legislativo 30 giugno 2003 n. 196, "Codice in materia di protezione dei dati personali" con particolare riferimento agli obblighi informativi a carico delle piccole e medie imprese" (in avanti, *Privacy* PMI). Inoltre è da segnalare che la misurazione non ha riguardato unicamente gli oneri associati agli obblighi informativi in senso stretto, ma anche gli oneri legati alle modalità di gestione delle informazioni associate a tali obblighi.

La struttura della "Scheda MOA"

Il documento si articola nei seguenti paragrafi:

1. *finalità e caratteristiche della normativa oggetto della misurazione*, in cui vengono presentati la *ratio* ed i contenuti principali della normativa i cui obblighi informativi sono oggetto di misurazione;
2. *mappatura degli obblighi informativi*, nel quale sono descritti gli obblighi informativi rintracciabili nella normativa;
3. *consultazione*, che illustra le modalità di coinvolgimento di *stakeholders* ed esperti,
4. *calcoli e stime degli oneri*, che illustra le scelte metodologiche associate alla determinazione dell'onere complessivo;
5. *proposte di semplificazione*, che indica alcuni possibili interventi di riforma.

[2] In accordo con la classificazione del modello EU SCM, la categoria nella quale rientra la normativa in esame è quella **B**: obblighi informativi che derivano da una norma comunitaria recepita nell'ordinamento nazionale.

1. FINALITÀ E CARATTERISTICHE DELLA NORMATIVA OGGETTO DELLA MISURAZIONE

La regolazione delle attività suscettibili di incidere sulla *privacy* è stata introdotta nel nostro ordinamento dalla legge 31 dicembre 1996, n. 675 ("Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali"), in risposta alle previsioni dell'accordo di Schengen che la ponevano come condizione per l'adesione; l'obiettivo della graduale abolizione dei controlli sulle persone alle frontiere comuni (e dunque la piena libertà di circolazione) veniva, infatti, perseguito nel rispetto delle libertà fondamentali e della dignità delle persone. La legge del 1996 (modificata nel 2001) recepiva, inoltre, la direttiva 1995/46/CE, "Tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati". La disciplina di riferimento è attualmente costituita dal decreto legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali" (di seguito, Codice), entrato in vigore il 1° gennaio 2004, che ha razionalizzato ed abrogato la normativa originaria.

Il Codice delinea una serie di regole comuni a tutti i trattamenti di dati, vale a dire a "*qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati*" (art. 4). L'uso personale è, invece, escluso dalla disciplina (art. 5, comma 3).

2. **MAPPATURA DEGLI OBBLIGHI INFORMATIVI**

La normativa oggetto della misurazione prevede nel complesso gli "*obblighi informativi*" (in avanti, O.I.) indicati di seguito.

O.I. n.01: **Informativa all'interessato e alla persona presso la quale sono raccolti i dati personali**

- **Fonte:** art. 13 del Codice; per la raccolta presso soggetti diversi dall'interessato, con le eccezioni di cui al comma 5 (trattamento per obbligo di legge, investigazioni difensive, sproporzione individuata dal Garante tra i mezzi necessari all'informativa e il diritto tutelato).
- **Soggetti obbligati**: imprese che trattano dati personali, con l'eccezione di cui sopra.
- **Obbligo informativo:** consiste nell'informativa anche orale sugli aspetti rilevanti del trattamento; consiste, altresì, nella conservazione del modulo di informativa indirizzata all'interessato ovvero nella affissione delle informazioni in luogo facilmente accessibile all'interessato, il tutto da esibire nel caso di controlli del Garante (che può servirsi della Guardia di Finanza).
- **Oggetto dell'obbligo informativo:** reperimento e comunicazione a terzi delle seguenti informazioni:

  - finalità e modalità del trattamento cui sono destinati i dati;
  - natura obbligatoria o facoltativa del conferimento dei dati;
  - conseguenze di un eventuale rifiuto di rispondere;
  - soggetti o categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l´ambito di diffusione dei dati medesimi;
  - diritti di cui all´articolo 7;
  - estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell´articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l´elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all´interessato in caso di esercizio dei diritti di cui all´articolo 7, è indicato tale responsabile.

- **Frequenza:** ogni volta che si acquisiscono dati personali, prima di chiedere il consenso se questo è necessario.
- **Relazione con i corrispondenti obblighi stabiliti in sede comunitaria:** la direttiva 95/46/CE impone l'utilizzo dell'O.I. "informativa all'interessato"; quanto all'oggetto, però, vi sono alcune differenze che aggravano gli oneri dell'impresa italiana:

  - mentre l'art. 10, co. 1, lettera c), terzo capoverso della direttiva prevede che l'informativa deve contenere l'indicazione dei diritti di accesso ai dati e rettifica "nella misura in cui, in considerazione delle specifiche circostanza in cui i dati vengono raccolti, tali informazioni siano necessarie per effettuare un trattamento leale nel confronto della persona interessata", nell'art. 13, co. 1,

lettera e) del Codice tale specificazione manca: le informazioni sul diritto all'accesso e alla rettifica devono essere fornite sempre;

- mentre l'art. 7, co. 2, lett. a) e d) del Codice prescrive che l'interessato ha diritto di ottenere dal responsabile del trattamento l'indicazione dell'origine dei dati e degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ex art. 5, comma 2, in base all'art. 12, co. 1, lett. a) della Direttiva 95/46/CE tali indicazioni non figurano tra quelle che l'interessato ha diritto a ricevere.

O.I. n. 02: **Consenso al trattamento dei dati personali**

- **Fonte:** art. 23 del Codice, con le eccezioni di cui all'art. 24 (adempimento di obblighi di legge o di contratto in cui è parte l'interessato, dati comunque conoscibili, ecc.).
- **Soggetti obbligati:** imprese che trattano dati personali (con le eccezioni di cui sopra).
- **Obbligo informativo e oggetto:** consiste nell'acquisizione del consenso dell'interessato al trattamento, che deve essere: espresso; dato liberamente; dato in forma specifica; preceduto da informativa (v. O.I. n. 1).
- **Frequenza:** prima di ogni trattamento (definito all'art. 4, primo comma, lett. a), ovvero di una o più operazioni di trattamento, di dati personali. [la stessa definizione è già a pag. 4]
- **Relazione con i corrispondenti obblighi stabiliti in sede comunitaria:** la direttiva 95/46/CE all'art. 7 prescrive la necessità del consenso, con le eccezioni che sono poi state riprodotte nel Codice (trattamento necessario per l'esecuzione di un contratto concluso con l'interessato, obblighi legali, salvaguardia dell'interesse vitale dell'interessato, esercizio di pubblici poteri ecc.): l'unica eccezione alla necessità del consenso non riprodotta in Italia che può essere di qualche interesse per la riduzione degli oneri delle imprese è: "(quando) è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano (sul) l'interesse o i diritti o le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell'art. 1, parag. 1".

O.I. n. 03: **Consenso al trattamento dei dati sensibili**

- **Fonte:** art. 26, primo comma del Codice, con le eccezioni di cui ai commi 3 e 4
- **Soggetti obbligati:** imprese che trattano dati sensibili (con le eccezioni di cui sopra).
- **Obbligo informativo e oggetto:** consiste nell'acquisizione e nella conservazione del consenso **scritto** dell'interessato al trattamento, che deve essere: espresso; dato liberamente; dato in forma specifica; preceduto da informativa (v. O.I. n. 1).
- **Frequenza:** prima di ogni trattamento (definito all'art. 4, primo comma, lettera a), ovvero di una o più operazioni di trattamento, di dati personali.
- **Relazione con i corrispondenti obblighi stabiliti in sede comunitaria:** per i dati personali "che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale", ovvero "relativi alla

salute o alla vita sessuale" (definizione coincidente con quella dell'art. 4 del Codice), l'art. 8 della direttiva 95/46/CE richiede il consenso *esplicito* al trattamento (e consente allo Stato di introdurre anche strumenti di controllo ulteriore), grosso modo con le medesime eccezioni riprodotte nel Codice. C'è dunque sostanziale conformità tra le due discipline.

O.I. n. 04: **Designazione (facoltativa) del responsabile del trattamento**

- **Fonte:** art. 29 del Codice.
- **Soggetti obbligati:** imprese i cui titolari non intendano occuparsi direttamente degli adempimenti in materia di privacy.
- **Obbligo informativo e oggetto:** designazione del responsabile del trattamento e individuazione analitica dei suoi compiti per iscritto, in un documento da conservare e produrre a richiesta del Garante.
- **Frequenza:** dipende dalla volontà del titolare del trattamento; la preposizione di un responsabile può essere relativa a tutti o solo ad alcuni dei trattamenti praticati dall'impresa.
- **Relazione con i corrispondenti obblighi stabiliti in sede comunitaria:** la direttiva 95/46/CE all'art. 2 parla di "responsabile del trattamento", che coincide con il "titolare del trattamento" di cui al Codice; e di "incaricato del trattamento" per indicare il soggetto che elabora dati personali per conto del responsabile del trattamento, che coincide con la corrispondente nozione del Codice (art. 30). La figura che il Codice descrive come "responsabile del trattamento", diverso dal titolare, non è contemplata.

O.I. n. 05: **Designazione (facoltativa) degli incaricati del trattamento**

- **Fonte:** art. 30 del Codice.
- **Soggetti obbligati:** imprese i cui titolari o responsabili del trattamento affidino ad incaricati lo svolgimento delle concrete operazioni di trattamento dei dati.
- **Obbligo informativo e oggetto:** designazione degli incaricati del trattamento e individuazione puntuale dell'ambito del trattamento consentito (ovvero: documentata predisposizione di una persona fisica a una unità per la quale è individuato per iscritto l'ambito del trattamento consentito agli addetti); i relativi documenti devo essere conservati e prodotti a richiesta del Garante.
- **Relazione con i corrispondenti obblighi stabiliti in sede comunitaria:** La designazione degli incaricati e gli adempimenti informativi connessi non sono formalizzati, ma è definito il principio (art. 16 Direttiva) che l'incaricato non elabori i dati ai quali abbia accesso, "se non dietro istruzione del responsabile del trattamento oppure in virtù di obblighi legali" e che l'incaricato "presenti garanzie sufficienti in merito alle misure di sicurezza tecnica e di organizzazione dei trattamenti da effettuare" (questa specificazione manca nel Codice, che dunque sul punto è meno oneroso della direttiva).

O.I. n. 06: **Misure minime di sicurezza nel caso di trattamento con strumenti elettronici (diverse dal DPS)**

- **Fonte:** artt. 33, 34, lett. da a) a f) e lett. h), e allegato B del Codice (punti da 1 a 18).
- **Soggetti obbligati:** imprese che trattano dati sensibili o giudiziari con strumenti elettronici.
- **Obbligo informativo:** provvedere agli adempimenti specificati ai punti da 1 a 18 dell'allegato B.
- **Oggetto dell'obbligo informativo:** predisporre un sistema di autenticazione informatica; procedure di gestione delle credenziali di autenticazione; eventuale autorizzazione degli incaricati; aggiornamento periodico dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o manutenzione degli strumenti elettronici; protezione degli strumenti elettronici rispetto a trattamenti illeciti e accessi non consentiti; adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.
- **Frequenza:** prima di procedere al trattamento; con cadenza almeno annuale va verificata la sussistenza delle condizioni di autorizzazione ed effettuato l'aggiornamento dell'ambito del trattamento; gli strumenti elettronici di protezione contro il rischio di intrusione vanno aggiornati con cadenza almeno semestrale; il salvataggio dei dati va effettuato con cadenza almeno settimanale.
- **Relazione con i corrispondenti obblighi stabiliti in sede comunitaria:** la direttiva 95/46/CE si limita ad assegnare agli Stati membri il compito di accertarsi che il responsabile del trattamento osservi le adeguate misure tecniche ed organizzative già al momento della progettazione del trattamento (cfr. considerando n. 46 e l'articolo 17) e parla di un generico "controllo preliminare sull'attività di trattamento di dati che presenti rischi specifici per i diritti e le libertà delle persone"; la norma comunitaria, più in generale, indica gli obiettivi da raggiungere (protezione dei dati dalla distruzione, alterazione, diffusione non autorizzata ecc.).

O.I. n. 07: **Tenuta del Documento programmatico per la sicurezza (DPS)**

- **Fonte:** artt. 33, 34, lett. g), e allegato B del Codice (punto 19).
- **Soggetti obbligati:** imprese che trattano dati sensibili o giudiziari con strumenti elettronici.
- **Obbligo informativo:** inserire nel DPS i contenuti indicati al punto 19 dell'All. B del Codice, nella Delibera 22.3.2004 del Garante e nella Guida operativa approntata dal Garante (che integra in modo specifico alcuni dei contenuti di legge).
- **Oggetto dell'obbligo informativo relativo al DPS:** reperimento delle informazioni riguardanti:

    - l'elenco dei trattamenti di dati personali;
    - la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
    - l'analisi dei rischi che incombono sui dati;

- le misure da adottare per l'integrità e la disponibilità dei dati e la protezione delle aree e dei locali;
- criteri e modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- interventi formativi degli incaricati del trattamento;
- i criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti affidati all'esterno della struttura;
- per i dati sanitari e idonei a rivelare la vita sessuale, l'individuazione dei criteri per la cifratura o la separazione dagli altri dati personali dell'interessato.

- **Frequenza:** entro il 31 marzo di ogni anno il DPS va redatto o aggiornato.
- **Relazione con i corrispondenti obblighi stabiliti in sede comunitaria:** si veda l'O.I. n. 06.

O.I. n. 08: **Indicazione nella Relazione accompagnatoria del bilancio di esercizio della avvenuta redazione o aggiornamento del DPS**

- **Fonte:** Punto 26 dell'allegato B del Codice; Delibera 22.3.2004 del Garante.
- **Soggetti obbligati:** imprese che trattano dati sensibili o giudiziari con strumenti elettronici e che siano tenute alla presentazione della relazione accompagnatoria del bilancio di esercizio.
- **Obbligo informativo e oggetto:** indicare nella relazione accompagnatoria al bilancio di esercizio se e quando il DPS è stato redatto o aggiornato.
- **Frequenza:** annuale, coincidente con la presentazione del bilancio di esercizio.
- **Relazione con i corrispondenti obblighi stabiliti in sede comunitaria:** si veda l'O.I. n. 06.

O.I. n. 09: **Misure minime di sicurezza nel caso di trattamento senza strumenti elettronici**

- **Fonte:** artt. 33, 35 del Codice.
- **Soggetti obbligati:** imprese che trattano dati personali senza l'utilizzo di strumenti elettronici.
- **Obbligo informativo:** provvedere agli adempimenti specificati ai punti da 27 a 29 dell'allegato B.
- **Oggetto dell'obbligo informativo:** predisporre le seguenti misure minime: aggiornamento periodico dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative; adozione di procedure idonee per la custodia dei documenti affidati agli incaricati; adozione di procedure per la conservazione degli atti in archivi ad accesso selezionato e con accesso che consenta l'identificazione degli incaricati.
- **Frequenza:** prima di procedere al trattamento; l'aggiornamento dell'ambito del trattamento va effettuato con cadenza almeno annuale.
- **Relazione con i corrispondenti obblighi stabiliti in sede comunitaria:** si veda l'O.I. n. 06.

O.I. n. 10: **Notificazione al Garante**

- **Fonte:** artt. 37 e 38 del Codice; fac-simile del modello di notificazione disponibile sul sito del Garante.
- **Soggetti obbligati:** imprese che effettuano il trattamento dei dati elencati all'art. 37 del Codice (modificato da provvedimenti del Garante come consentito dal comma 2).
- **Obbligo informativo:** trasmissione telematica di informazioni sul trattamento in base a un modello predisposto dal Garante, da sottoscrivere attraverso firma digitale (i soggetti non in possesso del dispositivo di firma digitale possono rivolgersi ad intermediari convenzionati). Per la prima notificazione, la modifica o la cessazione devono essere pagati diritti di segreteria pari a € 150 euro.
- **Oggetto dell'obbligo:** informazioni su tutti gli aspetti del trattamento (identità del titolare, del responsabile e degli incaricati, adozione delle misure minime di sicurezza, modalità del trasferimento dei dati all'estero ecc.): si veda il fac-simile sul sito (86 pagine).
- **Frequenza:** una sola volta, prima di procedere al trattamento dei dati; rinnovo nel caso di variazione dei dati riportati o di cessazione del trattamento.
- **Relazione con i corrispondenti oneri stabiliti in sede comunitaria:** l'art. 18 della direttiva 95/46/CE prevede lo specifico strumento della notificazione, per le medesime categorie di trattamenti (solo definite in negativo anziché in positivo come nel Codice), consentendo l'integrazione da parte delle Autorità nazionali; l'art. 19 definisce gli oggetti minimi che essa deve contenere; il fac-simile del Garante ne prevede molti di più; inoltre, l'art. 18, commi 4 e 5 della direttiva 95/46/CE consente agli Stati membri di prevedere modalità semplificate di notificazione, che il nostro legislatore non ha previsto. Infine, la direttiva non prevede il pagamento di diritti di segreteria.

O.I. n. 11: **Autorizzazione al trattamento di dati sensibili o giudiziari**

- **Fonte:** artt. 26, 40 e 41 del Codice; art. 11 DPR n. 501/98.
- **Soggetti obbligati:** imprese che trattano dati sensibili e la cui attività **non** è compresa fra quelle oggetto di una delle autorizzazioni generali del Garante sul tema del trattamento dei dati sensibili.
- **Obbligo informativo e oggetto:** compilazione di un modello (non ancora disponibile sul sito del Garante, per cui non è possibile dire quali obblighi informativi vadano in concreto assolti); il Garante può chiedere ulteriore documentazione. Vanno anche versati diritti di segreteria e considerate le eventuali spese postali (l'invio in formato elettronico non è l'unico consentito).
- **Frequenza**: una volta sola prima dell'inizio del trattamento
- **Relazione con i corrispondenti obblighi stabiliti in sede comunitaria:** l'art. 8 della direttiva 95/46/CE stabilisce un generale divieto di trattamento dei dati sensibili, ma, fra le eccezioni previste (oltre a quella del previo consenso descritta sopra), si consente, con le opportune garanzie, agli Stati membri di stabilire ulteriori deroghe a tale divieto, per motivi di interesse pubblico rilevante, sulla base della legislazione nazionale "o di una decisione dell'autorità di controllo": questo ultimo sembrerebbe il caso che il nostro legislatore ha specificato nelle ipotesi di autorizzazione. Inoltre, vale il principio che la direttiva enuncia all'art. 20, laddove impone un controllo preliminare dei trattamenti che

possono presentare rischi specifici per i diritti e le libertà delle persone, lasciando agli Stati la loro individuazione. Infine, la direttiva non prevede la corresponsione di diritti di segreteria.

Ai fini della misurazione degli oneri amministrativi, attraverso il questionario allegato, ,tra i sopraelencati obblighi informativi sono stati scelti, quelli che sono apparsi maggiormente **rilevanti**. La scelta effettuata ha tenuto conto anche delle segnalazioni delle associazioni di categoria emerse in sede di consultazione.

3. CONSULTAZIONE

Le informazioni necessarie per l'attività di misurazione sono state acquisite con una specifica attività di consultazione degli *stakeholders* che si è svolta in due diverse fasi e ha coinvolto diversi soggetti.

In primo luogo, sono state consultate le associazioni di categoria per identificare gli O.I. connessi alla regolazione in esame ritenuti più rilevanti per le imprese sotto il profilo degli oneri amministrativi. Inoltre, la consultazione degli *stakeholders* in questa fase ha permesso di definire la struttura del campione ragionato e di ottenere, in seguito, i nominativi delle imprese con le caratteristiche specificate alle quali somministrare il questionario.

In secondo luogo, la consultazione ha riguardato la rilevazione dei dati presso le imprese. In particolare, in questa fase, la consultazione è avvenuta secondo le seguenti modalità:

- ***Soggetti consultati***

  E' stato somministrato un questionario (in allegato), via fax e via e-mail, a un campione ragionato di imprese preventivamente contattate dalle associazioni di categoria che hanno risposto in un tempo che è andato dai due ai quattro giorni lavorativi [3]. Inoltre, sono stati consultati dei professionisti esperti (in particolare, ragionieri e dottori commercialisti, avvocati e consulenti del lavoro) in grado di fornire stime relative agli oneri amministrativi sostenuti dalle imprese di minori dimensioni per rispettare la normativa sulla *privacy*.

- ***Tecniche di consultazione adottate***

  Le tecniche di consultazione sono state differenziate in ragione delle caratteristiche dimensionali delle imprese, suddivise come segue.

  - Imprese con meno di dieci dipendenti. Sono stati consultati selezionati professionisti che offrono alle imprese servizi di consulenza specializzata sui temi oggetto della regolazione in esame al fine di ottenere indicazioni sul carico di lavoro e sui costi sostenuti dalle imprese appartenenti a questa classe dimensionale (*expert assessment*, nella metodologia SCM).
  - Imprese con almeno dieci dipendenti. Si è proceduto alla somministrazione del questionario, seguita da approfondimenti telefonici: le imprese sono state infatti ricontattate una volta ricevute le risposte, per chiarire alcune informazioni fornite e per raccogliere opinioni circa gli obblighi considerati più "irritanti".

[3] Il questionario è stato somministrato a 18 imprese: 16 imprese hanno restituito i questionari compilati, 14 dei quali contenevano risposte utilizzabili per la determinazione della stima degli oneri complessivi.

4. STIME DELL'ONERE SOSTENUTO DALLE IMPRESE PER ADEMPIERE AGLI OBBLIGHI INFORMATIVI *PRIVACY*

E' opportuno ricordare come le PMI siano un insieme di imprese molto numeroso in termini assoluti ed estremamente rilevante in termini di contributo al sistema economico e per numero di addetti L'universo delle PMI interessate dalla misurazione secondo i dati Istat, riferiti al numero delle imprese attive per almeno sei mesi e per classi di dipendenti è riportato nella seguente tabella (ISTAT, Archivio Statistico delle Imprese Attive [ASIA2004]).

DIPENDENTI	IMPRESE
1	3.459.969
2-9	643.422
10-249	171.078
Totale	**4.274.469**

Per il **calcolo** degli oneri amministrativi sono state seguite, come suggerito nei manuali sullo *Standard Cost Model* prodotti dalla Commissione e dai diversi paesi che hanno già utilizzato questo metodo, sono state seguite due vie distinte.

A. Per le **imprese al di sotto dei 10 dipendenti**, la stima degli oneri amministrativi sostenuti è stata effettuata sulla base delle indicazioni sul carico di lavoro e sui costi sostenuti, fornite da professionisti che offrono servizi di consulenza alle imprese in quest'ambito. Questa classe dimensionale, costituisce una popolazione di imprese estremamente eterogenea per settore di attività, capacità organizzativa e, in particolare, modalità di gestione dei dati e delle questioni amministrative, sono stati consultati alcuni professionisti esperti al fine di ottenere. Da questa ricognizione specifica, si evince che le principali differenze nei costi, legati all'adempimento degli obblighi previsti dalla normativa *privacy,* sembrano dipendere dal ricorso o meno, da parte della singola impresa, alla strumentazione elettronica. Ad esempio, l'uso del PC e del *software* applicativo per la gestione della documentazione relativa al consenso ai sensi delle norme sulla *privacy* costituisce un'aggravante soprattutto per le micro-imprese. Inoltre è rilevante, per le imprese con molti clienti e/o che svolgono attività che implicano il trattamento di dati sensibili, dovere o meno gestire le operazioni con personale interno dedicato.

B. Per le **imprese con almeno 10 dipendenti (**da 10 a 249 dipendenti)**,** la rilevazione degli oneri amministrativi dovuti alla normativa sulla *privacy* è consistita nella somministrazione di un questionario teso a misurare gli oneri che le imprese sostengono per rilevare, trattare e archiviare le informazioni richieste dalla normativa.

   In linea con la metodologia EU SCM e con le attività di rilevazione svolte anche da altri Paesi, il numero delle imprese intervistate è stato contenuto. Le

PMI erano tutte di dimensioni piuttosto eterogenee: nella scelta si è ritenuto opportuno individuare imprese attive in via prevalente in settori diversi (e che vanno dal turismo alla sanità, al recupero crediti, al settore manifatturiero). Tutte le imprese intervistate hanno mostrato un certo grado di consapevolezza delle problematiche connesse con il rispetto degli O.I. previsti dalla normativa. Inoltre, il campione ragionato delle imprese non è stato stratificato per dimensione a causa della scarsa numerosità delle imprese osservate nel corso della rilevazione. Limiti temporali hanno impedito una stima più disaggregata. I dati rilevati sono poi risultati molto variabili, anche a causa della varietà degli effetti prodotti, in termini di onerosità relativa, dal tipo degli obblighi informativi (paragrafo 2) nei diversi settori di attività considerati e in imprese così diverse per dimensione.Ciò premesso, è stata eseguita una serie di simulazioni per la stima dell'onere complessivo della *privacy*. Per il calcolo dell'onere complessivo finale sono stati utilizzati i valori mediani delle singole componenti di costo che, data l'estrema variabilità (tra le imprese intervistate) delle informazioni rilevate, risultano più robusti e, dunque, l'adozione di tale criterio (anche in ragione del numero limitato di unità osservate) consente di contenere gli effetti distorsivi indotti dal dato osservato sulla stima finale dell'onere. Inoltre, tale approccio metodologico offre una garanzia di protezione contro la presenza di dati anomali rispetto ad un approccio in cui la neutralizzazione dei dati anomali è affidata alla pura discrezionalità dell'analista.

Va poi segnalato come l'onere complessivo sia stato stimato come costo corrente annuale al netto di costi di adeguamento e capitale *una tantum*, che costituiscono la parte degli oneri di più difficile quantificazione da parte delle imprese, assumendo, inoltre, l'ipotesi di perfetta conformità delle imprese [4]. Sulla base di questa ipotesi, da considerarsi teorica, la stima dell'onere complessivo approssima il volume degli oneri effettivamente sostenuti dalle imprese dato che essi risulterebbero ragionevolmente simili a quelli calcolati nell'esercizio svolto in assenza di evasione degli obblighi imposti dalla regolamentazione della *privacy*. Infine va ricordato che, anche se l'onere è stato rilevato al netto dei costi che le imprese avrebbero sostenuto comunque per finalità diverse dalla normativa sulla *privacy*, ciò non esclude la possibilità che taluni oneri determinino effetti anche 'produttivi' in senso lato, ovvero contribuiscano al miglioramento gestionale – ad esempio – delle procedure di trattamento dei dati interne o generino ricadute aziendali positive in termini di organizzazione del lavoro.

I singoli obblighi informativi specifici sono risultati tutti complessivamente alquanto rilevanti in termini di oneri amministrativi. Gli oneri più rilevanti sono connessi, in particolare, con la trasmissione e conservazione dell'informativa relativa ai dati personali, l'informativa relativa ai dati personali ed il trattamento dei dati senza strumenti elettronici. Nella fase di consultazione è emerso che l'obbligo di redazione del DPS, indipendentemente dai suoi costi, è considerato come particolarmente sproporzionato rispetto alle caratteristiche delle organizzazioni sulle quali ricade.

[4] L'ipotesi di perfetta conformità, in ultima analisi, fa crescere le stime. Essa è generalmente adottata dai paesi che usano lo SCM, oltre che dalla Commissione. L'alternativa, in assenza di rilevazioni specifiche e approfondite sul livello di rispetto della normativa, sarebbe ipotizzare arbitrariamente la percentuale di non conformità, ma questa non è sembrata una soluzione ragionevole.

L’onere complessivo annuale calcolato con la metodologia sopra indicata (punti A e B) è pari a **1.752 MILIONI DI EURO**.

5. PROPOSTE DI SEMPLIFICAZIONE

Alla luce dell'entità dell'onere stimato e di una approfondita analisi della normativa, in questa sezione si espongono sinteticamente alcune proposte di semplificazione che, in linea con le previsioni comunitarie ed i principi ispiratori del Codice, consentirebbero di alleggerire gli obblighi e gli oneri per le imprese. In particolare, le proposte si riferiscono a:

DATI PERSONALI

Escludere dai "dati personali" le informazioni relative alle persone giuridiche, gli enti e le associazioni (art. 4, comma 1, lett. b) del Codice)

La direttiva 95/46 si riferisce ai soli dati appartenenti a "persone fisiche" (art. 2, lett. a)). Con l'intervento in parola, le imprese non dovrebbero più preoccuparsi di sottoporre al regime del Codice i dati di imprese, enti e associazioni con le quali vengono in contatto, i quali non godrebbero più dei diritti sanciti nel Codice. Oltre all'Italia, solo l'Austria e il Lussemburgo (dati del 2002), tra i Paesi europei, risultano avere optato per questa estensione. Questa discrepanza, tra l'altro, crea problemi nei rapporti transnazionali fra imprese, in quanto ad es. un'impresa francese non si aspetta che un'impresa o un ente italiano possa esercitare i diritti relativi alla tutela dei propri dati personali, e viceversa

DATI SENSIBILI

Escludere dai dati "sensibili" l'informazione della malattia resa dal dipendente al datore di lavoro, senza indicazione della patologia (cioè la sola prognosi, contenente l'indicazione dell'inizio e della data presunta dell'infermità, con esclusione della diagnosi, cioè della specifica malattia del dipendente).

Consentirebbe alle imprese che non trattano dati sensibili di evitare di chiedere il consenso dei dipendenti al trattamento di questi dati, con la conseguente redazione del documento programmatico per la sicurezza e l'adozione delle misure di sicurezza più stringenti previste nel Codice. Anche la recente delibera del Garante 23 novembre 2006, n. 53, "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 privato" conferma l'inclusione anche della mera "prognosi" nella categoria dei dati sensibili, disponendo che il datore di lavoro abbia accesso solo a questa e non anche alla diagnosi.

RESPONSABILE E INCARICATO DEL TRATTAMENTO

Ammettere che la preposizione del responsabile e dell'incaricato del trattamento (artt. 29, comma 4 e 30, comma 2, del Codice) possa essere orale o comunque provata per testimoni nel caso di contestazioni.

L'intervento è compatibile con la direttiva 95/46/CE che non conosce la figura del "responsabile del trattamento" e non prevede la preposizione per iscritto dell'incaricato.

INFORMATIVA ALL'INTERESSATO

Escludere dall'oggetto dell'informativa l'indicazione dell'origine dei dati (art. 13, comma 1, lettera e), 7, comma 2, lettera a) del Codice).

L'intervento riconduce l'oggetto dell'informativa a quello minimo previsto dalla direttiva: infatti, mentre l'art. 7, co. 2, lett. a) e d) del Codice prescrive che l'interessato ha diritto di ottenere dal responsabile del trattamento l'indicazione dell'origine dei dati e degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ex art. 5, comma 2, in base all'art. 12, co. 1, lett. a) della Direttiva 95/46/CE tali indicazioni non figurano tra quelle che l'interessato ha diritto a ricevere.

CONSENSO

Eliminare l'obbligo di consenso scritto (art. 23, comma 3, del Codice).

A termini della Direttiva, il consenso deve essere "espresso" (art. 7, comma 1, lettera a) della Direttiva) e può dunque, in caso di contestazioni, essere provato per testimoni. La necessità di un consenso scritto sembra essere una particolarità italiana; la legge del Regno Unito addirittura non definisce il consenso e alcune disposizioni fanno presumere che, in alcuni casi, esso possa essere "implicito" (*implied consent*). Solo in Italia e in Germania la legge sulla *privacy* determina anche le caratteristiche del modulo con il quale il consenso deve essere raccolto (dati del 2002).

DOCUMENTO PROGRAMMATICO PER LA SICUREZZA (DPS)

Sostituire, per le piccole imprese, l'obbligo di tenuta del DPS con un adempimento semplificato, disciplinato da apposita delibera del Garante.

Lo strumento specifico del DPS non è imposto dalla normativa europea; si possono studiare strumenti maggiormente coerenti con il principio della proporzionalità dell'onere rispetto alle dimensioni dell'impresa, i quali, trovando fonte in una delibera del Garante, sarebbero anche meglio adattabili al progredire della tecnologia.

NOTIFICAZIONE

Eliminare dalle informazioni richieste nel modulo della notificazione al Garante e delineate nel fac-simile per la notificazione telematica pubblicato sul sito del Garante, tutto quanto è già contenuto nel documento programmatico sulla sicurezza, rinviando al medesimo, che si può allegare oppure esibire a richiesta.

Va notato che i dati soggetti a notificazione (genetici, patrimoniali ecc.) sono un sottoinsieme di quelli (sensibili e giudiziari) il cui trattamento elettronico fa scattare l'obbligo di redazione del DPS: ne consegue che le imprese tenute alla notificazione sono in massima parte, se non *in toto*, soggette all'obbligo di DPS (resta fuori la categoria, ormai virtuale, delle imprese che trattano dati genetici, patrimoniali ecc. SENZA strumenti elettronici). In questo modo si evita alle imprese l'onere di riempire le 86 pagine del modulo per la notificazione presente sul sito del Garante.

Del resto i trattamenti “non automatici” (quindi non elettronici) ai sensi dell’art. 18 della Direttiva non dovrebbero nemmeno essere soggetti a notificazione: l’inclusione di tale categoria nell’ambito della notificazione è una particolarità di alcune soltanto delle legislazioni nazionali in materia (Italia, Grecia, Danimarca, Lussemburgo, Portogallo, dati del 2002).

Eliminare dalle informazioni richieste in sede di notificazione quanto non strettamente previsto dalla direttiva.

Rispetto alle altre legislazioni nazionali, quella italiana richiede che il notificante renda un gran numero di informazioni: ad es. in ordine al luogo del trattamento, alle sue modalità tecniche, all’interconnessione dei dati.

ALLEGATO

QUESTIONARIO DI RILEVAZIONE