



Consorzio per lo Sviluppo  
delle Metodologie e delle Innovazioni  
nelle Pubbliche Amministrazioni

# **BANCHE DATI E TUTELA DELLA PRIVACY NELLE PUBBLICHE AMMINISTRAZIONI**

I primi risultati di una ricerca interdisciplinare

A cura di G. Comandé

n. 3 - 2001



## **BANCHE DATI E TUTELA DELLA PRIVACY NELLE PUBBLICHE AMMINISTRAZIONI**

I primi risultati di una ricerca interdisciplinare

**n. 3 - 2001**

Istituto Nazionale di Statistica  
via Cesare Balbo, 16 - Roma

MIPA  
Consorzio per lo Sviluppo delle Metodologie e Innovazione  
nelle Pubbliche Amministrazioni  
via Alessandria, 195 - Roma

*Coordinamento editoriale:*  
Servizio Produzione Editoriale  
via Tuscolana, 1788 - Roma

*Fotocomposizione*  
*P. Lucantoni*

*Stampa:*  
ISTAT - Centro stampa  
via Tuscolana, 1788 - Roma  
Settembre 2001

*Copie:* 400

Contributi di Elisabetta Bani, Giovanni Comandé, Beatrice Pieraccini, Paolo Bizzarri



# INDICE

INTRODUZIONE	7
PARTE PRIMA - Banche dati e tutela della privacy nelle Pubbliche Amministrazioni: profili giuridici ed esperienze pratiche	15
1. Premessa al lavoro svolto	15
2. I termini del problema	17
3. Le normative sull'accesso	18
4. (segue) Le normative sull'accesso	21
5. (segue) Le normative sull'accesso	24
6. Il processo di informatizzazione della pubblica amministrazione	26
7. Breve excursus del processo di informatizzazione della pubblica amministrazione	27
8. La Rete Unitaria della Pubblica Amministrazione e il documento amministrativo elettronico	28
9. La normativa sul trattamento dei dati personali	31
10. (segue) La normativa sul trattamento dei dati personali	35
11. I problemi ancora aperti	37
12. Il lavoro svolto	39
13. La metodologia seguita	40
14. I primi risultati	41

GLOSSARIO	49
PARTE SECONDA - Banche dati e tutela della privacy nelle Pubbliche Amministrazioni: profili tecnici ed esperienze pratiche	51
1. Premessa al lavoro svolto	51
2. I termini del problema	53
3. Gli standard internazionali sulla sicurezza informatica	54
4. Lo standard ITSEC	55
4.1 <i>La struttura dello standard ITSEC</i>	55
4.2 <i>L'obiettivo di sicurezza</i>	56
4.3 <i>La valutazione dell'efficacia</i>	58
4.4 <i>La valutazione della correttezza</i>	59
5. L'uso dello standard ITSEC nella PA	60
6. I problemi aperti	61
Normative Statali	63

# INTRODUZIONE

Sotto il profilo metodologico la ricerca è stata svolta avvalendosi di esperti appartenenti a discipline diverse.

In tale approccio interdisciplinare il confronto delle soluzioni giuridiche con le possibilità tecniche, e quindi il dialogo tra giuristi ed informatici, ha rappresentato un momento qualificante. In tal modo si sono potuti definire i problemi e le politiche di sicurezza per la corretta gestione del rischio in imprese pubbliche nella gestione di dati sensibili dal punto di vista della privacy e soprattutto si è irrobustita una capacità di dialogo tra le competenze che si rivelerà decisiva per eventuali ulteriori sviluppi del presente lavoro.

Non casualmente l'obiettivo principale del progetto di ricerca consisteva nel promuovere la collaborazione ed il dialogo tra competenze diverse, in particolare tra giuristi ed informatici, onde raggiungere un grado di comprensione delle problematiche esaminate più approfondito e completo. Il percorso tracciato non vedeva semplicemente la redazione di elaborati distinti ed attinenti a competenze diverse quanto il coordinato sviluppo della comprensione delle problematiche così che i profili giuridici potessero essere ben osservati ed eventualmente affrontati sul piano tecnico-informatico e viceversa le soluzioni tecniche fossero compatibili con le previsioni giuridiche ed in grado di soddisfarne le esigenze prospettate.

Questo aspetto del progetto sperimentale è stato quello che ha richiesto i maggiori sforzi ed il maggior impegno di tempo, anche se i ricercatori impegnati avevano avviato su altri argomenti e su altri settori ricerche che si sono rivelate estremamente produttive in termini di risultati grazie all'applicazione di questa metodologia di lavoro.

Al di là di una sola apparente distinzione in due parti dei contributi sotto il profilo del linguaggio tecnico prevalente (giuridico o tecnico-informatico), la ricerca e la scelta delle aree di disciplina da approfondire così come l'analisi degli standard di sicurezza e della loro possibile corrispondenza con i requisiti (minimi) imposti da leggi o da regolamenti si sono avvalse del continuo confronto tra le competenze coinvolte.

Del resto, i temi affrontati presentano elevati tassi di innovazione e di complessità già per ciascuna delle competenze impiegate. Infatti, la ricerca ha rivelato elevati tassi di innovazione tecnologica e normativa ad un tempo, spesso tra loro in disaccordo, ed elevati livelli di complessità soprattutto sotto il profilo normativo giacché gli approdi più recenti del legislatore sovrappongono o, meglio, più spesso affiancano regolamentazioni di origine comunitaria a normative, ed a linee di indirizzo politico, sedimentatesi nel tempo.

Peraltro, alcune delle normative approvate più di recente presupponevano già operato un cambio di mentalità e di cultura sulla mera base dell'approvazione, negli anni precedenti di norme di indirizzo o di dettaglio che verso tale mutata mentalità avrebbero dovuto orientare le pubbliche amministrazioni.

A tal proposito un esempio tra tutti quelli emersi sarà sufficiente: già con l'art. 3 del D.lgs. 12 febbraio 1993, n. 39, in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, il nostro ordinamento prevedeva che: "gli atti amministrativi adottati da tutte le pubbliche amministrazioni sono di norma predisposti tramite sistemi informativi automatizzati". A questa predisposizione informatizzata, addirittura automatizzata degli atti, però, continuava a fare da riscontro una realtà in cui l'informatizzazione al massimo corrispondeva alla sostituzione delle macchine da scrivere con dei più moderni sistemi di videoscrittura.

Al gap di tipo normativo, e per molti aspetti di tipo tecnologico come le considerazioni in tema di adeguamento agli standard ITSEC mettono impietosamente a nudo, si affiancava un ancora più grave gap culturale di comprensione piena e diffusa della portata innovativa che l'informatizzazione, nel senso più pieno e moderno del termine, poteva offrire sia per velocizzare l'attività delle PPA.A. sia per introdurre crescenti elementi di efficienza nel sistema.

Al contempo, però, le innovazioni tecnologiche che si affacciavano sulla scena non solo "promettevano" questi risultati ma consentivano di dare più facile risposta ad altri "diritti" che nel frattempo erano stati riconosciuti.

L'allusione, in primo luogo, rinvia al più agevole ed economico accesso agli atti della P.A. che oltre a garantire una maggiore partecipazione del cittadino alle attività procedurali che lo riguardano, dovrebbe produrre un maggiore livello di controllo di questo sulla P.A. stessa e quindi un maggior livello di controllo diffuso della P.A. il che dovrebbe generare maggiori efficienze.

Il processo fin qui tracciato rimane estremamente positivo a dispetto delle difficoltà di implementazione prima sommariamente enunciate e che verranno approfondite nella trattazione.

Tuttavia, il quadro viene reso ancora più complesso e difficilmente gestibile quando iniziano a considerarsi altri profili che, in qualche modo, fanno da "contraltare" rispetto a quelli serviti in senso ampio dall'accesso all'attività della P.A. da parte del soggetto interessato. Assai di frequente, infatti, un procedimento dovrà "trattare" ai sensi della legge n. 675/1996 dati riguardanti soggetti diversi dall'interessato che esercita il suo diritto all'accesso. In questi casi, le amministrazioni sono tenute al rispetto di entrambe le normative che impongono cautele ed obblighi diversi a seconda dell'oggetto del trattamento e della fonte che permette il trattamento da parte della P.A.. In alcuni casi si tratterà di un obbligo imposto dalla legge, altre volte sarà un trattamento consentito perché funzionale al perseguimento delle finalità. In ogni caso il "livello" di accessibilità varierà in relazione ai contenuti, al soggetto pubblico che tratta i dati, al soggetto cui i dati si riferiscono ed al soggetto che a questi dati voglia accedere, al tempo dell'accesso ed alle sue modalità, se esso si accompagni o meno alla possibilità di estrazione di copia e così di seguito.

In questo quadro assai frammentario e per molti aspetti confuso, il punto di partenza per la scelta della normativa di riferimento da selezionare e da studiare è stato inevitabilmente l'orientamento più recente del legislatore. Si è rilevato, infatti, un orientamento volto a potenziare il ruolo delle regioni e degli enti locali, aumentandone competenze e funzioni, in ossequio a un'ottica "decentralista" ormai condivisa. Motore di tale processo sono state le c.d. leggi Bassanini e quelle di attuazione alle medesime. Con l'attuazione della legge 15 marzo 1997, n. 59 funzioni e compiti amministrativi dello Stato sono stati conferiti (o lo saranno a breve termine) alle regioni ed agli enti locali.

L'esercizio delle nuove competenze implica, tra le altre cose, la gestione di un ingente quantitativo di informazioni, sia che ciò venga imposto in maniera espressa dalla legge con obblighi alla costituzione di banche dati o di sistemi informativi, sia che discenda implicitamente dal conferimento delle nuove funzioni, come modo ottimale per esercitarle.

Tali soggetti pubblici si trovano o si troveranno ben presto a dover approntare adeguate procedure informatiche o ad organizzare nuove banche dati per l'assolvimento dei nuovi compiti. L'impostazione e la gestione di tali nuove banche dati si dovrà realizzare in un momento in cui gli stessi soggetti sono già in difficoltà a gestire le banche dati esistenti e ad adeguare ai nuovi principi espressi dalla legge n. 675/96 i procedimenti amministrativi di loro competenza.

In generale può affermarsi che in capo alle amministrazioni pubbliche si prospettano nuovi diritti-doveri a informare e a essere informate con corrispondenti esigenze di sicurezza informatica e di temperamento delle diverse situazioni soggettive interessate.

Segnatamente il diritto all'informazione e di accesso alla documentazione amministrativa riconosciuto in capo al cittadino-utente si traduce in un'inevitabile dovere di informazione (cd. dissemination dei dati) a carico della Pubblica Amministrazione, che garantisca contestualmente il diritto di partecipazione alla vita politica e sociale, il principio di trasparenza del pubblico potere, operando, però, in modo "che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale" (art. 1 comma 1 legge n. 675/1996).

Le modifiche intercorse nella logica e, in parte, nella disciplina dell'accesso agli atti hanno contribuito fortemente a trasformare nella sostanza l'accesso agli atti in un accesso alle informazioni in possesso delle pubbliche amministrazioni imponendo di mutare la logica di analisi e di intervento. In definitiva mentre prima un atto era o meno accessibile oggi le amministrazioni non solo devono verificare, per così dire in generale, l'accessibilità del documento ma poi devono pure agire selettivamente sull'atto in astratto accessibile per temperare le diverse "pretese" sulle informazioni in esse contenute e dalla P.A. detenute a titolo, fin e con limiti diversi.

Appaiono subito intuitivamente chiare le innumerevoli difficoltà incontrate nel conciliare e temperare questa disciplina nel suo concreto esercizio con le realtà dinamiche delle pubbliche amministrazioni, specialmente negli enti locali.

Alla crescita delle possibilità e delle necessità di accesso per ragioni economiche, di efficienza, di semplificazione, tecnologiche si contrappongono, però, i maggiori vincoli anche normativi connessi alla tutela delle persone nel trattamento dei dati personali. Alle problematiche legate alla riservatezza ed al segreto delle PPAA. si affiancano quelle relative

alla riservatezza delle persone soprattutto nel loro rapportarsi con l'accesso ai dati in possesso di queste amministrazioni. I profili organizzativi classici, le finalità e la gestione delle informazioni, siano o meno contenute in banche dati tradizionali, la legittimità delle operazioni di raccolta e trattamento, non sono più i soli aspetti salienti da considerare. Anzi questi stessi aspetti vengono (devono essere) visti in prospettiva dinamica per vedere come reagiscono ed interagiscono con le esigenze di tutela della riservatezza.

Sotto altro punto di vista - quello dell'essere informati - la P.A. deve poter disporre di tutta una serie di informazioni necessarie all'esercizio delle nuove funzioni, talvolta specificate, come accennato, nelle normative più recenti ma assai più spesso "genericamente" rientranti nelle normali funzioni della P.A.

Per fare qualche esempio, il recente D.lgs. 23 dicembre 1997 n. 469 - di attuazione alla c.d. legge Bassanini uno -, con cui sono state conferite alle regioni e agli enti locali funzioni e compiti in materia di mercato del lavoro, prevede l'istituzione di un sistema informativo lavoro, denominato S.I.L., a cui Ministero del lavoro, regioni ed enti locali hanno l'obbligo di connettersi per scambiare dati, secondo le modalità indicate su parere dell'AIPA. A tale banca dati possono accedere, previa la stipula di convenzioni apposite, anche soggetti privati quali le imprese di fornitura di lavoro interinale.

Su un piano più generale e sempre esemplificando, la Conferenza Stato regioni deve approvare protocolli di intesa per la costituzione di banche dati per l'interscambio di dati e informazioni sull'attività posta in essere dalle amministrazioni centrali, regionali e delle province autonome (D.lgs. 28 agosto 1997, n. 281).

A tal ultimo proposito deve essere segnalato che molte regioni si sono già attivate per la formazione di proprie reti telematiche, che collegano, all'interno, tutti i soggetti amministrativi tra loro e, all'esterno, questi con l'amministrazione centrale dello Stato (AIPA), e a volte anche con la rete Internet, in modo da essere universalmente accessibili. Così la Toscana, che ha di recente approvato il piano di indirizzo per l'attuazione della rete telematica regionale, così la Sicilia, la cui assemblea regionale ha realizzato un sito web in cui è disponibile tutto il proprio sistema informativo (dalle leggi regionali, ai disegni di legge alle sentenze dei TAR siciliani e del Consiglio di Giustizia amministrativa).

Lo sforzo informatico che incombe sulle pubbliche amministrazioni è evidente: qualcosa è stato fatto, molto rimane da fare, sia in ottemperanza alle numerose normative che prevedono tali obblighi, sia per meglio gestire

le proprie funzioni, quindi per meglio "amministrare" ed offrire servizi.

Queste considerazioni ampiamente dibattute nel corso dell'indagine hanno consentito di sperimentare e poi scartare per gradi di approssimazione successivi diverse possibili impostazioni della ricerca e della classificazione del materiale normativo portando a concludere per l'adozione di un criterio "contenutistico" distinguendo le normative in due grandi gruppi, banche dati statali, da una parte, regionali e locali, dall'altra, soddisfacendo, però, in parte anche il criterio "soggettivistico" alla luce delle diverse responsabilità che gli enti territoriali stanno andando ad assumere ed in prospettiva evolutiva assumeranno.

Ciò ha consentito di apprezzare opportunamente pure le differenze tra apparato statale e apparato periferico, o meglio, le omogeneità, dal momento che si è potuta riscontrare una sostanziale corrispondenza nella previsione di informatizzazione, così da poter essere in definitiva stimolata l'interconnessione.

È proprio tenendo sempre ben presente l'evoluzione tracciata del complesso universo informativo della pubblica amministrazione sempre più orientato a costituire una rete di banche dati interconnesse, che l'analisi si è concentrata sul temperamento dei diritti di accesso (e gli obblighi di disseminazione delle informazioni) e della riservatezza intesa sia nel senso del "segreto" dell'amministrazione sia della tutela dei soggetti coinvolti nel trattamento dei dati visti nel prisma delle moderne problematiche della sicurezza informatica.

In questa chiave si è cercato, in via di prima approssimazione, di enucleare i problemi che gli enti pubblici devono affrontare, con particolare attenzione sulla capacità di definire politiche di sicurezza appropriate nella gestione dei propri sistemi informatici, appropriate sia sotto il profilo tecnico-giuridico che tecnico-informatico. Da un punto di vista tecnico giuridico tali politiche devono rispondere ad un insieme di requisiti fortemente contrastanti:

- favorire la trasparenza dell'ente pubblico nei confronti dell'esterno;
- favorire l'integrazione in rete con altri sistemi della P.A. (progetto di rete unitaria della pubblica amministrazione);
- fornire al cittadino garanzie sul corretto utilizzo dei propri dati personali.

Da un punto di vista tecnico-informatico i requisiti che devono essere soddisfatti presentano due differenti aspetti: uno di carattere strettamente tecnico e l'altro di compatibilità delle soluzioni tecnologiche con i criteri e i livelli prospettati a livello normativo. Se il primo presuppone il

riconoscimento delle proprietà solo negative e probabilistiche della sicurezza informatica, il secondo profilo non ammette deviazioni o alternative dall'essere o dal non essere in "regola" con la disciplina di legge.

Proprio in questa direzione e con questi caveat lo studio delle problematiche prima evidenziate è stato svolto procedendo ad una compiuta e coordinata lettura delle normative che impongono obblighi di informatizzazione alla P.A. con particolare riferimento agli enti locali per le ragioni specificate e secondo la logica indicata.

Si è altresì proceduto ad una analoga lettura delle norme che impongono obblighi all'informazione, sia attiva che passiva, che possono essere meglio attuati tramite l'informatizzazione.

Infine, è stata approntata la base informativa per verificare la compatibilità dei nascenti sistemi informatici con la normativa sulla privacy e le relative decisioni del Garante.

Dall'analisi compiuta emerge come il progetto della R.U.P.A. sia un'opportunità e al contempo un luogo di incontro per le problematiche qui trattate e di passaggio da una logica in cui la computerizzazione del vecchio dominava ad un momento in cui l'informatizzazione rivoluziona ed innova le procedure.

Il momento di innovazione drammaticamente accelerata che ci si trova a governare impone tempi di reazione estremamente rapidi e chiara progettualità che non ci è sembrato di potere pienamente rilevare quantomeno in un tema, quello della sicurezza, che rappresenta un ideale crocevia di queste problematiche, sia dal punto di vista della circolazione interna delle informazioni che della vulnerabilità esterna del sistema.

La progettualità di rapida innovazione tecnologica e, soprattutto di svecchiamento delle conoscenze da parte delle risorse umane dovrebbe quindi tenere conto del fatto che l'informatizzazione della P.A. ha semplificato l'azione amministrativa ma ha pure accresciuto le possibilità di accesso alle informazioni in possesso della P.A. di fatto cogliendo l'organizzazione, le strutture tecniche e lo stesso quadro normativo in uno stato di preoccupante arretratezza. Ciò non tanto, o non solo, perché manchino idonee discipline, quanto perché esse possono rimanere pericolosi monumenti ad un'innovazione sulla carta che può rivelarsi "di carta".

L'auspicio che emerge, dunque, è che almeno gli enti locali regolamentino unitariamente la gestione delle informazioni in loro possesso, elaborando regolamenti o linee guida a vantaggio sia dei dipendenti pubblici che dei cittadini stimolando così una competizione sui servizi e sulla qualità degli

stessi. Sarebbe peraltro auspicabile una disciplina organica della gestione delle informazioni in possesso della P.A. in grado di fornire una base minima, anche a livello di misure e standard di sicurezza, sui quali poi possa articolarsi l'accennata competizione sulla qualità dei servizi informatizzati offerti.

Ciò, inoltre, contribuirebbe in modo assai penetrante a definire il potere informatico della P.A.: i dati che una P.A. si trova a trattare, le banche dati di sua gestione, quelle a cui è interconnessa.

In questa direzione il risultato più tangibile della ricerca forse è l'elaborazione di un quadro tipo sinottico in cui poter inserire le singole banche dati per mettere in rilievo i loro aspetti più significativi rendendone immediatamente percepibile la natura e il funzionamento.

In prospettiva di riorganizzazione e sistematizzazione del complesso informativo della P.A., e non solo, la scheda predisposta costituisce poi un importante momento di avvio per un'analisi volta a tipizzare le banche dati.

# PARTE PRIMA

## BANCHE DATI E TUTELA DELLA PRIVACY NELLE PUBBLICHE AMMINISTRAZIONI: PROFILI GIURIDICI ED ESPERIENZE PRATICHE

1. Premessa al lavoro svolto - 2. I termini del problema - 3. Le normative sull'accesso - 4. (segue) Le normative sull'accesso - 5. (segue) Le normative sull'accesso - 6. Il processo di informatizzazione della pubblica amministrazione - 7. Breve excursus del processo di informatizzazione della pubblica amministrazione - 8. La Rete Unitaria della Pubblica Amministrazione e il documento amministrativo elettronico - 9. La normativa sul trattamento dei dati personali - 10. (segue) La normativa sul trattamento dei dati personali - 11. I problemi ancora aperti - 12. Il lavoro svolto - 13. La metodologia seguita - 14. I primi risultati.

### **1. Premessa al lavoro svolto**

Con il presente lavoro si è cercato di avviare un riordino critico e ragionato dell'ingente normativa che concerne l'informatizzazione della P.A. nell'ottica di disporre di una base conoscitiva il più possibile certa per il conseguimento degli obiettivi prefissati nel progetto di ricerca.

La valutazione della compatibilità tra il processo di informatizzazione delle pubbliche amministrazioni con le esigenze scaturite dalla normativa sulla privacy passa di necessità da un chiarimento preliminare di cosa e quanto

è stato e deve essere ancora informatizzato.

Le attività della P.A. che implicano la gestione di informazioni sono numerose ed eterogenee, potendo anzi affermarsi che l'attività amministrativa si sostanzia quasi inevitabilmente nella raccolta di informazioni, a volte anche con la partecipazione degli stessi amministrati.

Risulta infatti difficile immaginare un documento amministrativo che non contenga informazioni e queste informazioni attengono per lo più a persone fisiche o giuridiche.

E' inoltre probabile, e non infrequente, che negli "archivi" della P.A. siano contenuti dati eccedenti rispetto alle finalità di raccolta, per cui si pone un problema di verifica della sussistenza dei presupposti indicati dalla legge o dal regolamento per quella specifica raccolta dati e un adeguamento ai nuovi parametri normativi, che potrebbe portare a una ricognizione e revisione dei criteri di tenuta di molti elenchi pubblici.

D'altra parte il programma generale di riordino della P.A. e di semplificazione amministrativa ed il processo di informatizzazione della pubblica amministrazione hanno condotto al conseguimento di traguardi ritenuti impensabili fino a pochi anni fa: basti pensare alla cosiddetta "teleamministrazione", ovvero a quel sistema caratterizzato dal fatto che interventi di uffici o amministrazioni diversi da quelli che devono emettere l'atto finale sono esercitati a distanza, su di un'unica pratica impostata presso il centro elaborazione dati di chi deve emettere l'atto finale.

L'ultima meta raggiunta è stata il riconoscimento della validità giuridica dell'atto in forma elettronica, ex art. 15, secondo comma, della legge 15 marzo 1997, n. 59, che ha riconosciuto, a tutti gli effetti di legge, la validità e la rilevanza giuridica degli atti, dati e documenti formati dalla P.A. e dai privati con strumenti informatici o telematici, dei contratti stipulati nelle medesime forme nonché della loro archiviazione e trasmissione con strumenti informatici. La disposizione è stata poi attuata con il regolamento adottato con D.P.R. 10 novembre 1997, n. 513 contenente, tra l'altro, la definizione di documento informatico e la disciplina della firma digitale, nonché dalle disposizioni in materia di protocollo elettronico dettate dal regolamento per la gestione del protocollo informatico (D.P.R. n. 428/98) e dalle regole tecniche per la formazione, trasmissione, conservazione, duplicazione, riproduzione e validazione dei documenti informatici ( D.P.C.M. 8 febbraio 1999).

E' agevole notare che questo ingente quantitativo di informazioni o "dati" gestito dalle amministrazioni tramite banche dati, registri, archivi, sistemi informativi, ecc. non solleva di per sé alcuna questione particolare, se non

nel momento in cui si provvede a garantirne l'accesso al cittadino utente, in osservanza delle leggi 6 giugno 1990, n. 142 e 7 agosto 1990, n. 241.

Con l'accesso si pone infatti in essere un'attività di comunicazione e di diffusione di dati che deve necessariamente conformarsi con le esigenze di riservatezza sottese alla legge 31 dicembre 1996, n. 675.

In particolare la cospicua attività amministrativa di comunicazione e di diffusione di dati avviene sia con l'accesso alle informazioni da parte degli interessati, ai sensi, come detto, delle leggi nn. 142 e 241 del 1990, sia con la pubblicazione degli atti, ma mentre in questo secondo caso si agisce per lo più in attuazione di leggi o regolamenti ed è quindi disciplinata dall'art. 27 della legge n. 675, nel primo caso occorre verificare di volta in volta la compatibilità tra le due normative.

## **2. I termini del problema**

Sono quindi privacy e accesso i poli da conciliare, ovvero delle disposizioni dettate in momenti storici diversi, a tutela di interessi disomogenei e concernenti ambiti oggettivi solo in parte coincidenti.

Come la dottrina ha ormai più volte rilevato, infatti, le due normative si sovrappongono, ma non coincidono, poiché hanno, ad esempio, un diverso ambito oggettivo (quella sull'accesso si riferisce ai documenti e agli atti amministrativi, quella sulla riservatezza ai dati personali) e una diversa connotazione giuridica (la legge n. 241/90 è una legge di principio, la legge n. 675/96 una legge che contiene "disposizioni generali").

Già prima dell'entrata in vigore della legge n. 675/96, invero, si era tentato di trovare un punto di equilibrio tra le esigenze di trasparenza e pubblicità e quelle di tutela della riservatezza. L'art. 24, secondo comma, lett. d, della legge n. 241/90 e l'art. 8 del regolamento attuativo, D.P.R. 27 giugno 1992, n. 352 - dove si parla esplicitamente di riservatezza - provvedono a disciplinare il diritto di accesso nel caso in cui la richiesta riguardi documenti contenenti informazioni riservate. Tuttavia detta previsione normativa, a causa della sua indeterminatezza, non fornisce soluzioni, bensì opera un mero rinvio a un giudizio di merito riservato alla P.A., che deve valutare quale delle due esigenze, trasparenza o privacy, prevalga.

Come meglio vedremo in seguito, infatti, la possibilità di sottrarre determinati documenti all'accesso per motivi di riservatezza è demandato ai regolamenti delle singole amministrazioni, alle quali spetta, nell'ambito ovviamente dei

(generici) principi stabiliti dalla legge e dal regolamento di attuazione, il compito di canonizzare il contemperamento degli interessi in parola.

L'entrata in vigore della legge n. 675/96, infine, facendo salve in quanto compatibili le norme della legge n. 241/90, pone proprio il problema di stabilire i limiti di tale compatibilità

Sul punto si sono inevitabilmente formati orientamenti discordanti e la letteratura e la giurisprudenza in materia sono ormai copiose. In particolare la giurisprudenza amministrativa ha tentato in vario modo di fissare dei "picchetti" alla questione. Si possono ricordare a mero titolo di esempio le pronunce del Consiglio di Stato che, nel caso di conflitto tra accesso e riservatezza, risolvono limitando l'accesso alla sola visione dell'atto, senza consentirne l'estrazione di copia (tra le tante Cons. Stato, sez. IV, 29 gennaio 1998, n. 115 in Foro amm. 1998, n. 32); oppure quelle che ritengono prevalente l'accesso sulle esigenze di privacy ogniqualvolta venga in rilievo per il richiedente la cura o la difesa di propri interessi (tra le tante Cons. Stato, sez. IV, 24 marzo 1998, n. 498, in Cons. St. 1998, I, 373; Cons. Stato ad. plen. 4 febbraio 1997, n. 5, in Giur. It. 1997, III, 1, 249); o ancora quelle che consentono al concorrente di una procedura concorsuale l'accesso e la copia degli elaborati anche degli altri candidati per il necessario giudizio di relazione intercorrente con essi (Cons. Stato, sez. IV, 11 gennaio 1994, n. 21, in Riv. Amm. Rep. It. 1994, n. 788).

Le prime pronunce del Garante tuttavia avallano l'interpretazione secondo cui il regime della legge n. 241 sopravviva integralmente all'entrata in vigore della legge n. 675.

### **3. Le normative sull'accesso**

A fronte di tali problematiche e partendo da esse, sembra opportuno fare un passo indietro per verificare come, nel periodo di applicazione che va dall'emanazione ad oggi, è stata interpretata e applicata la normativa sull'accesso, sia dalla dottrina sia dalla giurisprudenza, sottolineandone i passaggi più significativi ai fini della presente indagine.

In particolare si vuole verificare, partendo dalla lettera della legge e dall'interpretazione a essa data, se ci sono aperture in cui poter inquadrare le esigenze della privacy, così come individuate e disciplinate dalla legge n. 675, o se, all'opposto, la normativa sull'accesso presenta pericolose chiusure - perché conferisce un eccessivo potere discrezionale alla P.A. nel

valutare la possibilità dell'accesso o perché delinea essa stessa dei contorni troppo estesi per l'accesso ma l'ipotesi è remota - alle medesime esigenze.

Come noto (art. 22, primo comma, legge n. 241), ha diritto di accesso chiunque presenti "un interesse per la tutela di situazioni giuridicamente rilevanti", qualunque soggetto, cioè, qualificato dall'essere portatore di una situazione giuridica di vantaggio, da tutelare tramite l'accesso a determinate informazioni.

In sede regolamentare il D.P.R. n. 352/92 ha aggiunto che tale interesse deve essere personale e concreto. Per quanto detta qualificazione (personalità e concretezza) echeggi la terminologia processualistica, laddove vengono fissate le condizioni dell'agire processuale, è pacifico che il legislatore del 1990 ha inteso attribuire una connotazione più ampia alle parole usate, rendendo corrispondentemente più esteso il ventaglio dei soggetti legittimati a chiedere l'accesso.

Come ha infatti sottolineato la giurisprudenza (tra le tante Consiglio Stato, sez. V, 7 marzo 1997, n. 228, in Cons. Stato, 1997, I, n. 361) la presenza dell'interesse è necessaria solo per verificare l'esistenza di una correlazione tra esso e il contenuto della pretesa di conoscenza.

Su questo piano, pertanto, non è possibile interpretare l'art. 22, primo comma, come selettore dell'accesso alla luce della normativa sulla privacy: non è in altre parole possibile inferire, facendo leva sul richiamato interesse, limitazioni soggettive all'accesso, a pena di stravolgere il dettato della legge 241/90 e di consentire rifiuti ingiustificati, rinnegando, in nome della privacy, le finalità di trasparenza e di imparzialità della pubblica amministrazione.

E' stata parimenti adottata una interpretazione estensiva anche per l'art. 22, secondo comma, laddove viene definito il "documento amministrativo" del quale è consentito l'accesso: andando oltre la già ampia nozione fornita dalla lettera della legge ("è considerato documento amministrativo ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa") la giurisprudenza amministrativa ha considerato documenti amministrativi anche gli atti interni della P.A., nonché gli atti di diritto privato finalizzati alla cura concreta di interessi della collettività.

E' stato infatti ritenuto che il diritto di accesso sia correlato, più che agli atti, all'attività della pubblica amministrazione, per cui esso deve essere esercitato nei confronti degli atti esterni e interni afferenti all'attività di diritto amministrativo e di diritto privato che sia volta alla cura concreta di interessi

della collettività (ex plurimis, Cons. Stato 15 gennaio 1998, n. 14, in Foro amm., 1998, n. 26).

Pertanto, resta esclusa la sola attività di diritto privato che, per quanto esercitata da una pubblica amministrazione, sia del tutto svincolata dall'interesse pubblico istituzionalmente preposto alle attività della P.A.

Da ciò ne consegue la presenza di un ulteriore elemento di possibile conflitto tra gli interessi di cui ci occupiamo, accesso e privacy: si pensi al caso in cui un cittadino chiede l'accesso al contratto di appalto stipulato tra l'amministrazione e un privato già aggiudicatario di una gara pubblica; il soggetto, si ripete, chiede l'accesso, non agli atti della gara, bensì al disciplinare stipulato contrattualmente tra P.A. e privato. Quid juris? E' legittimato il privato a conoscere i dettagli dell'accordo raggiunto?

Per quanto riguarda questi aspetti, ovvero l'estensione del diritto di accesso, occorre prendere in considerazione anche la legge 142/90, che, all'art. 7, nell'enunciare il diritto dei cittadini ad accedere agli atti amministrativi, alle informazioni e alle strutture e ai servizi degli enti locali, delinea un accesso dai connotati più estesi rispetto alla legge 241/90.

Segnatamente l'art. 7 prescrive che, con regolamento comunale e provinciale, viene assicurato ai cittadini, singoli e associati, il diritto di accesso agli atti amministrativi, previa individuazione, con norme di organizzazione degli uffici e dei servizi, dei responsabili dei procedimenti.

A tal fine il regolamento deve anche dettare "le norme necessarie per assicurare ai cittadini l'informazione sullo stato degli atti e delle procedure e sull'ordine di esame di domande, progetti e provvedimenti che comunque li riguardano", nonché deve assicurare "il diritto dei cittadini di accedere, in generale, alle informazioni di cui è in possesso l'amministrazione".

Il quinto comma, infine, prevede che, allo scopo di rendere effettiva la partecipazione dei cittadini all'attività dell'amministrazione, gli enti locali assicurano l'accesso alle strutture ed ai servizi agli enti, alle organizzazioni di volontariato e alle associazioni.

Viene pertanto a configurarsi, come detto, un diritto di accesso dai confini più estesi rispetto a quello delineato nella legge 241/90, soprattutto laddove si fa riferimento all'accesso alle informazioni, o meglio, a tutte le "informazioni di cui è in possesso l'amministrazione".

Si tratta evidentemente di qualcosa di più dell'accesso agli atti, anche se sembra invero difficile ipotizzare un'informazione, di cui si chieda l'accesso, che non sia contenuta in un atto o che sia accessibile prescindendo da un supporto cartaceo o informatico.

Nondimeno il Comune e la Provincia sono assoggettati a questo obbligo di informazione in senso esteso, che deve essere attuato a livello regolamentare: sarà dunque in questa sede, ancora una volta, che la massima garanzia della trasparenza e della partecipazione alla vita amministrativa (quantomai avvertita negli enti locali, istituzionalmente vicini al cittadino) dovrà trovare contemperamento con la tutela della sfera privata dei terzi, anch'essi potenzialmente più esposti in un contesto territoriale limitato e "conosciuto".

#### **4. (segue) Le normative sull'accesso**

Proseguendo in questa disamina critica della normativa sull'accesso, l'art. 8, quinto comma, del regolamento n. 352/92, a cui si è già accennato, prevede le ipotesi di esclusione del diritto di accesso, i casi, cioè, in cui esso non è ab origine esercitabile, essendo ostacolato da esigenze di "segretezza", intesa in senso lato.

Come visto, l'ultima delle ipotesi in considerazione (lett. d) esclude l'accesso nel caso in cui i documenti riguardino "la vita privata o la riservatezza di persone fisiche, di persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all'amministrazione dagli stessi soggetti cui si riferiscono".

Tale previsione merita un qualche approfondimento, anche se potrebbe ritenersi superata dalle più ampie previsioni della legge 675/96.

Innanzitutto viene in considerazione la necessità che degli interessi attinenti alla riservatezza - elencati, si ritiene, in via esemplificativa - i soggetti siano in concreto titolari.

Con tale specificazione, evidentemente, si richiede, ai fini della tutela, la non eventualità dell'interesse, la sua attualità, la possibilità di individuarlo con precisione proprio nell'aspetto della titolarità.

Sembra emergere una preoccupazione del legislatore di veder circoscrivere o negare il diritto all'informazione, ogniqualvolta venga paventata l'esistenza di un interesse alla riservatezza.

In questo contesto può essere inquadrato anche l'ulteriore inciso della lettera d): "deve comunque essere garantita ai richiedenti la visione degli atti dei procedimenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i loro stessi interessi giuridici".

E' immediatamente percepibile come la lettera di questa previsione sia stata successivamente mutuata dalla giurisprudenza amministrativa per affermare la prevalenza del diritto all'accesso sulle esigenze di riservatezza laddove "venga in rilievo per il richiedente la cura o la difesa di propri interessi" (cfr. le già richiamate sentenze Cons. Stato, sez. IV, 24 marzo 1998, n. 498, in Cons. Stato, 1998, I, n. 373; Cons. Stato, ad. plen., 4 febbraio 1997, n. 5, in Giur. It., 1997, III, 1, n. 249).

Tuttavia tale formulazione non chiarisce cosa succede qualora il richiedente, dopo aver preso visione del documento, ravvisi la necessità di produrlo in un eventuale giudizio proprio al fine di curare e difendere i suoi interessi giuridici: in tal caso, infatti, il regolamento 352/92 non concede la possibilità di estrazione di una copia, dovendosi pertanto auspicare una previsione di dettaglio nei regolamenti delle singole amministrazioni.

Deve inoltre essere segnalato che la dottrina ha aggiunto un ulteriore requisito per l'esercizio del diritto di accesso nel caso di compresenza di esigenze connesse alla riservatezza: oltre alla titolarità concreta dell'interesse, deve essere altresì necessario, nel senso di indispensabile, il ricorso all'accesso per l'esplicazione della tutela dell'interesse giuridico; si richiede, in altre parole, che il titolare del diritto di accesso debba provare che, per tutelare il proprio interesse giuridico, non esiste altra via se non l'accesso a quelle particolari informazioni detenute dall'amministrazione.

Anche nella legge n. 142/90 è presente un riferimento alla riservatezza.

L'art. 7, terzo comma, prevede che "tutti gli atti dell'amministrazione comunale e provinciale sono pubblici, ad eccezione di quelli riservati per espressa indicazione di legge o per effetto di una temporanea e motivata dichiarazione del Sindaco o del Presidente della Provincia che ne vieti l'esibizione, conformemente a quanto previsto dal regolamento, in quanto la loro diffusione possa pregiudicare il diritto alla riservatezza delle persone, dei gruppi o delle imprese".

E' agevole notare che, mentre nella legge 241/90 la tutela della riservatezza può negare in radice o differire il diritto di accesso (con prevalenza del differimento sul diniego ove possibile, art. 8, terzo comma DPR 352/92), nella legge 142/90 la medesima esigenza comporta un divieto temporaneo e motivato dell'accesso, e non una sua preclusione.

La sottrazione all'accesso è invece prevista, nella legge 142/90, nei soli casi di documenti riservati per legge.

Per quanto concerne il citato "differimento" della legge 241/90, l'art. 24 conferisce facoltà alle pubbliche amministrazioni, soggette ex art. 23, alla

disciplina della 241/90, di differire l'accesso fino a quando la conoscenza dei documenti possa impedire od ostacolare gravemente lo svolgimento dell'azione amministrativa.

Si tratta di un mero rinvio temporale, a cui potrebbe anche seguire un diniego di accesso. Una tale decisione deve essere motivata, ai sensi dell'art. 7 del regolamento attuativo, in maniera particolarmente stringente, dovendo il responsabile del procedimento fare specifico riferimento alla normativa vigente, alle categorie di documenti sottratti all'accesso, individuati dalle amministrazioni ai sensi dell'art. 24, quarto comma, della legge 241/90, alle circostanze di fatto per cui la richiesta non può essere accolta così come proposta.

Il regolamento, come accennato, prevede il differimento, oltre che per la tutela degli interessi citati nella legge 241/90, per salvaguardare esigenze di riservatezza dell'amministrazione, specie nella fase preparatoria dei provvedimenti, in relazione a documenti la cui conoscenza possa compromettere il buon andamento dell'azione amministrativa.

Tornano, pertanto, in considerazione le esigenze relative alla tutela della riservatezza, ma riferita, stavolta, all'amministrazione stessa, che può tutelare la propria "privacy" differendo l'accesso.

Sorvolando sull'opportunità di parlare di riservatezza con riferimento a una pubblica amministrazione, si assiste qui al singolare caso in cui accesso e riservatezza non fanno capo, come di norma, a soggetti distinti tra cui l'amministrazione funge da tramite, in un rapporto di tipo trilaterale, bensì a due soggetti, l'uno portatore del diritto all'informazione e l'altro obbligato a fornire l'informazione e contestualmente legittimato a tutelare, tramite la negazione o il differimento dell'accesso, la propria riservatezza.

Sembra di poter affermare che in questo duplice ruolo l'amministrazione possa perdere la propria istituzionale imparzialità, per la possibilità che le viene offerta di trincerarsi dietro le esigenze di privacy al fine di negare il diritto del cittadino. Si verrebbe pertanto ad assistere a un'ipotesi di conflitto tra accesso e privacy diversa da quella sinora prospettata e potenzialmente più iniqua, sia per i potenziali esiti, sia per la posizione di privilegio in cui viene a trovarsi la P.A. rispetto al cittadino.

Un'applicazione fedele del dettato normativo in tema di motivazione e di finalità del differimento possono però scongiurare tale pericolo, che, invero, non ha mai dato adito a pronunce giurisprudenziali di significativo rilievo.

## 5. (segue) Le normative sull'accesso

Ulteriori considerazioni possono farsi sull'art. 5, terzo comma, del regolamento n. 352/92.

Qui viene prevista l'ipotesi, più frequente di quanto possa crederci, che l'atto di cui è consentito l'accesso richiami altri atti o documenti, che sono collegati con il primo.

La norma richiamata prevede la facoltà di accedere anche agli altri documenti, purché appartenenti al medesimo procedimento, fatte salve le eccezioni stabilite dalla legge o dal regolamento.

Onde evitare il verificarsi di una sorta di automatismo nel consentire l'accesso anche ai documenti "connessi", sembra necessario reinterpretare tale norma alla luce delle esigenze di privacy, che - qualora non siano (ancora) recepite in sede di regolamento delle singole amministrazioni - dovranno operare da freno allo scattare del meccanismo di "accesso a catena" ipotizzato dalla normativa.

L'art. 5, sesto comma, del regolamento prevede poi che l'esame dei documenti di cui sia stato consentito l'accesso possa essere effettuato dal richiedente o da persona da lui incaricata con l'eventuale accompagnamento di altra persona di cui vanno specificate le generalità, che devono essere poi registrate in calce alla richiesta.

L'eventuale presenza di una o più persone al momento della visione del documento amministrativo - di cui vengano (solo) registrate le generalità - potrebbe inficiare il controllo che la P.A. svolge sull'esercizio del diritto di accesso da parte del cittadino tramite la richiesta di motivazione: può, in altre parole, prendere visione del documento chi non presenta un interesse rilevante e quindi acceda per mera curiosità, ipotesi negata dalla giurisprudenza (Cons. Stato, sez. V, 14 aprile 1997, n. 362, in *Foro amm.*, 1997, 1095, laddove si afferma che "l'interesse che legittima la richiesta ... di accesso... deve essere personale, concreto, serio, non emulativo, né riconducibile a mera curiosità, oltreché ricollegabile alla persona dell'istante..., da uno specifico nesso sia contenutistico, sia temporale...").

Si ponga il caso di chi accede agli atti di un procedimento concorsuale per averne preso parte, rispetto a chi non essendo né candidato né aspirante a un concorso non presenta alcun interesse a ingerirsi nella legittimità o illegittimità degli atti che sono per lui improduttivi di conseguenze sfavorevoli o favorevoli, e presenta ancor meno interesse alla conoscenza delle valutazioni di merito a cui sono andati soggetti i singoli candidati (per un

caso giurisprudenziale di questo genere cfr. Tar Campania, sez. I, 23 febbraio 1995, n. 38 in *Foro amm.*, 1995, 1358).

Tali considerazioni impongono pertanto, all'interprete, o meglio al legislatore, un ripensamento dell'attuale formulazione dell'art. 5, sesto comma, del DPR n. 352/92 alla luce delle esigenze della privacy.

Sul piano organizzativo, l'art. 6 del citato regolamento prevede che "le singole amministrazioni individuano un ufficio che fornisca tutte le informazioni sul diritto di accesso e sugli eventuali costi", eventualmente istituendo, su valutazione discrezionale della amministrazione, un ufficio di relazioni con il pubblico.

Inoltre l'art. 4, settimo comma, prevede un responsabile del procedimento di accesso nella persona del dirigente o, su designazione di questi, di un altro dipendente addetto all'unità organizzativa competente a formare l'atto o a detenerlo stabilmente.

Parimenti la legge 142/90 prevede all'art. 7, quarto comma, che l'amministrazione locale individui, con norme di organizzazione degli uffici e dei servizi, i responsabili dei procedimenti.

Vi è da chiedersi come si coordineranno all'interno delle singole amministrazioni queste disposizioni con quelle sulla privacy, laddove sono previste le figure del responsabile e dell'incaricato del trattamento, se sarà possibile e opportuno cumulare su un unico soggetto più compiti o se invece dovranno essere individuati soggetti distinti, a cui affidare in via esclusiva tali funzioni oppure a cui attribuire nuove e ulteriori mansioni.

Ultime considerazioni sono da svolgere sull'art. 25, quinto comma, della legge 241/90, laddove si prevede la tutela giurisdizionale del diritto d'accesso tramite quel ricorso speciale proponibile in sede di giurisdizione esclusiva al Tribunale Amministrativo Regionale entro 30 giorni dalla determinazione concernente il diritto di accesso e discusso e deciso in Camera di Consiglio nei trenta giorni dalla scadenza del termine per il deposito del ricorso. Abbreviato a trenta giorni è anche il termine per fare appello al Consiglio di Stato.

Orbene, l'espressione usata "contro le determinazioni amministrative concernenti il diritto di accesso" è stata interpretata, in dottrina, nel senso di consentire l'azione giurisdizionale anche contro le decisioni che abbiano accordato l'accesso: ne deriva una possibilità per il singolo che si veda leso dal riconoscimento a terzi del diritto di visione di documenti che lo riguardino, di insorgere contro tale accesso, beneficiando della disciplina

processuale accelerata della norma in esame.

A tal proposito la giurisprudenza, partendo dalla considerazione che tra i beni per la cui salvaguardia può essere escluso il diritto di accesso l'art. 24 della legge 241/90 ha posto la riservatezza dei terzi, ha ritenuto che costoro, (che siano persone, gruppi o imprese) hanno titolo ad opporsi al giudizio per l'accesso ex art. 25 legge 241/90, quali controinteressati.

In particolare essi possono far valere, a esclusiva tutela della loro riservatezza: in primo luogo la mancanza di legittimazione in senso assoluto dell'istante; in secondo luogo l'infondatezza della pretesa azionata da parte di quei soggetti che, pur legittimati ad agire, non siano, in concreto, attualmente titolari di interessi giuridici da curare; in terzo luogo la limitazione del diritto d'accesso alla sola visione degli atti (Tar Lazio, sez. III, 5 maggio 1995, n. 772, in TAR, 1995, I, 2158).

Da ciò a maggior ragione può derivarsi l'esistenza di un diritto di azione autonomo in capo al soggetto, la cui riservatezza sia stata lesa dall'accesso a documenti consentito ad altri.

## **6. Il processo di informatizzazione della pubblica amministrazione**

Descritte a grandi linee le caratteristiche più salienti del quadro normativo e giurisprudenziale in materia di accesso, sembra a questo punto opportuno spendere qualche parola sul processo di informatizzazione della pubblica amministrazione.

Non è infatti pensabile allo stato attuale analizzare l'insieme delle regole che presidono alla circolazione delle informazioni all'interno della P.A. e tra questa ed il cittadino senza tenere nel debito conto il livello di informatizzazione e di interconnessione raggiunto dalla P.A.

L'accesso agli atti amministrativi è possibile in misura massiccia solo attraverso una strumentazione che consenta di riprodurre, archiviare, far circolare con economicità e semplicità le informazioni. Non a caso la stessa legge 241/90 dà una definizione di documento amministrativo che ricomprende anche il documento amministrativo elettronico.

L'interazione tra la legge 241/90 e il processo di informatizzazione si attesta anche su un altro piano: la semplificazione amministrativa, a cui la legge 241/90 è, com'è noto, finalizzata, viene senza dubbio favorita dall'informatizzazione, laddove questa incrementa la capacità di dialogo tra le amministrazioni, rendendo di conseguenza più rapida e semplice la

circolazione di dati detenuti da singole amministrazioni.

Vi è però da segnalare che le amministrazioni pubbliche si sono mosse solo di recente in direzione del processo di informatizzazione, ciò ha comportato un ritardo sia nell'acquisizione dei vantaggi sopradescritti, sia anche nel porsi e nell'affrontare gli inevitabili problemi di ordine tecnico e giuridico che ne scaturiscono.

Molte sono pertanto le problematiche ancora aperte, a tutto ciò dovendosi poi aggiungere la questione della compatibilità di tale contesto con la legge sul trattamento dei dati personali.

## **7. Breve excursus del processo di informatizzazione della pubblica amministrazione**

Per decenni l'informatizzazione dell'amministrazione ha significato semplicemente l'acquisto materiale di strumenti informatici, trascurando di sfruttare le nuove possibilità offerte dai sistemi informatici e, invece, applicando ai nuovi sistemi computerizzati, le vecchie procedure. I nuovi strumenti sono stati usati per esigenze gestionali (soprattutto per la contabilità e la gestione del personale) e ciò che è stato a lungo trascurato sono stati l'aspetto dei rapporti tra amministrazioni diverse ed il problema dei rapporti con il cittadino.

Non si deve dimenticare che l'informatizzazione amministrativa ha preso l'avvio intorno alla fine degli anni sessanta senza una base normativa adeguata: l'unico riferimento normativo è stato per anni (anni nei quali le amministrazioni cominciavano a dotarsi dei primi strumenti informatici) la circolare della Presidenza del Consiglio dei Ministri 6 marzo 1968, n. 465.1.12 "per il coordinamento delle attività dei centri meccanografici ed elettronici presso le amministrazioni statali".

Solo a partire dal 1980 il Provveditorato Generale dello Stato ha emanato una serie di circolari relative alla progettazione, realizzazione e gestione dei sistemi informativi automatizzati.

Si trattava comunque di discipline dirette a regolare gli acquisti e la gestione dei sistemi informativi automatizzati, non quindi quell'insieme di attività che oggi si definisce trattamento dei dati.

In particolare negli anni '80-'90 ci si è cominciati a preoccupare del problema dell'informatizzazione, soprattutto per ciò che riguarda gli aspetti di compatibilità tecnica tra sistemi informativi.

Un qualche cenno al trattamento dei dati si può invece rintracciare nella

disciplina sul sistema statistico nazionale e nelle leggi istitutive di alcune banche dati, ma si tratta di discipline embrionali, settoriali e rispondenti a mere contingenze.

Un ruolo più significativo è stato svolto in quegli anni dalle regioni e dagli enti locali, che, pur nel circoscritto ambito in cui hanno potuto gestire l'informatizzazione, hanno dato prova di maggiori capacità programmatiche e organizzative.

Non a caso in ambito regionale troviamo una cospicua "legislazione sommersa", relativa alla gestione delle banche dati, anche se le singole normative non fanno riferimento, nei titoli e nelle rubriche, all'informatica propriamente detta.

E' proprio in ambito regionale, ad esempio, che vengono sperimentati i primi modelli di programmazione: la legge regionale Emilia Romagna 26 luglio 1988, n. 30, recante "Costituzione del sistema informativo regionale" traccia un'ampia prospettiva di interventi e di controlli di carattere amministrativo e finanziario per promuovere un sistema informativo regionale.

In questo contesto troviamo affrontato anche il problema della tutela della riservatezza nell'acquisizione, trattamento e diffusione dei dati personali. Vengono infatti elencate le cautele necessarie; viene disciplinato il diritto dei privati ad ottenere le informazioni concernenti la propria persona e ad ottenere gratuitamente la correzione di eventuali errori od omissioni. Viene addirittura introdotto, all'art. 5 della citata legge, una sorta di garante regionale per i dati statistici. ("Il Presidente della giunta regionale con proprio decreto individua il dirigente responsabile della adozione delle procedure per il segreto statistico, della riservatezza dei dati e delle misure che assicurino l'acquisizione, validazione e trasmissione all'ISTAT e alle Amministrazioni centrali dello Stato dei dati dovuti").

## **8. La Rete Unitaria della Pubblica Amministrazione e il documento amministrativo elettronico**

Una tappa ben più significativa, per l'ambito nazionale in cui è collocata, è rappresentata dalla realizzazione della Rete Unitaria della Pubblica Amministrazione, progetto entrato nella fase operativa a seguito dell'approvazione da parte del Consiglio dei ministri della direttiva del 5 settembre 1995 (che recepisce le indicazioni presentate dall'AIPA al Governo), a seguito della quale è stato realizzato dall'AIPA uno studio di

fattibilità conclusosi il 31 gennaio 1996 (prima dell'entrata in vigore della legge 675/96).

La realizzazione della RUPA consente al sistema informativo di ciascuna amministrazione l'accesso ai dati ed alle procedure esistenti nei sistemi informativi delle altre. Anche nella realizzazione di questo progetto occorre valutare la compatibilità del sistema con la normativa in materia di diritto di accesso (di segreto) e di tutela della riservatezza (dei diritti del singolo rispetto al trattamento dei dati personali).

La Rete infatti dovrebbe consentire alle singole amministrazioni di colloquiare tra di loro per lo scambio di documenti ed informazioni e di conseguenza dovrebbe rappresentare per la collettività un centro unitario di erogazione di dati e prestazioni amministrative.

Spetta all'AIPA verificarne il livello di sicurezza, dovendo prevedere norme tecniche e regolamentari per la protezione dei dati, mentre ogni singola amministrazione resterà responsabile delle proprie banche dati e delle informazioni ivi contenute. La RUPA infatti ha una struttura di cosiddetta "rete di reti", per cui ogni amministrazione continua a gestire in modo autonomo i propri dati attraverso una rete privata confluyente nella rete unica.

Per quanto concerne il documento amministrativo elettronico, che è figlio del processo di informatizzazione, i primi tentativi di riconoscimento della forma informatica di alcuni procedimenti si riscontrano nella legge 27 febbraio 1985, n. 52 che, in occasione della meccanizzazione delle conservatorie dei registri immobiliari, all'art. 16 autorizza, per l'iscrizione dell'ipoteca, la presentazione di una nota (in sostituzione della nota in doppio originale ex art. 2659, I co, c.c.) redatta su supporto informatico o la sua trasmissione mediante l'uso di elaboratori elettronici e prevede (art. 29, VI comma) la possibilità per gli utenti di procedere ad ispezione dei registri mediante interrogazioni a distanza direttamente sugli elaboratori elettronici usati dalle conservatorie.

Come visto, la definizione di documento amministrativo dell'art. 22 della legge n. 241/90 comprende anche quella di documento elettronico, essendone pertanto previsto l'accesso, al pari degli altri tipi di documento.

Del resto il futuro delle attività della pubblica amministrazione è destinato a essere caratterizzato in misura prevalente dalla automatizzazione, se è vero che l'art. 3 del D.lgs. 12 febbraio 1993, n. 39, in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, ha stabilito che: "gli atti amministrativi adottati da tutte le pubbliche amministrazioni sono di norma predisposti tramite sistemi informativi automatizzati".

Inoltre viene anche previsto che nell'ambito delle pubbliche amministrazioni

l'immissione, la riproduzione su qualunque supporto e la trasmissione di dati, informazioni e documenti mediante sistemi informatici o telematici, nonché l'emanazione di atti amministrativi mediante i medesimi sistemi, devono essere accompagnati dall'indicazione della fonte e del responsabile dell'immissione, riproduzione trasmissione o emanazione. Se per la validità di tali operazioni e degli atti emessi è prevista l'apposizione di firma autografa, la stessa è sostituita dall'indicazione a stampa, sul documento prodotto dal sistema automatizzato, del nominativo del soggetto responsabile.

L'ultimo significativo intervento del legislatore nella nostra materia si è avuto con la legge 15 marzo 1997, n. 59 (Bassanini 1) e con il D.P.R. 10 novembre 1997, n. 513, intitolato "Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'art. 15, comma 2, della legge 15 marzo 1997, n. 59". Segnatamente il regolamento affronta il problema della paternità dell'atto introducendo e disciplinando la cosiddetta firma digitale.

Ovviamente deve essere garantita la riservatezza delle informazioni contenute nel documento informatico e questa passa attraverso la definizione dei criteri di sicurezza dei dati informatici, che devono essere immutabili ed inalterabili.

Le amministrazioni, nel dare attuazione alla disciplina sul documento informatico, dovranno affrontare anche il problema della tutela della riservatezza da un duplice punto di vista: dovranno adottare tutte le misure necessarie a garantire la protezione dei dati trattati da invadenze esterne e dovranno regolamentare e proteggere la circolazione dei dati al proprio interno.

E' infatti eloquente a questo proposito l'art. 3, quarto comma, del D.P.R. n. 513 che lascia "fermo quanto previsto dall'art. 15 della legge 31 dicembre 1996, n. 675".

Come è noto la definizione dei criteri di sicurezza è amplissima e deve essere aggiornata periodicamente, con decorrenza almeno biennale per aggiornarsi alle innovazioni dettate dal progresso tecnologico. L'art. 15 della legge 675/96 dispone infatti che i dati oggetto di trattamento devono essere custoditi e controllati anche in relazione alle conoscenze acquisite grazie al progresso tecnologico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza i rischi di accesso non autorizzato e di trattamento non conforme alle finalità della raccolta.

Questa digressione ci è sembrata doverosa alla luce del fatto che è dal combinato disposto delle due discipline che viene determinata la

regolamentazione del documento elettronico: significativamente, al fine di garantire il cittadino dai rischi di utilizzo indebito di informazioni riservate e di accesso abusivo alle stesse, l'applicazione della normativa sul documento informatico è stata subordinata all'emanazione delle apposite regole tecniche per la tutela della riservatezza.

## 9. La normativa sul trattamento dei dati personali

Passiamo ora ad affrontare nel dettaglio la normativa sul trattamento dei dati personali, legge 31 dicembre 1996, n. 675, analizzandone, al solito, gli aspetti più significativi per le finalità di questo lavoro.

In questa ottica un articolo chiave della normativa *de qua* è l'art. 27, a cui si è accennato in premessa, che disciplina il trattamento di dati personali effettuato da soggetti pubblici, prendendo in esame sia la comunicazione e la diffusione di tali dati a soggetti pubblici, sia la loro comunicazione e diffusione da parte di tali soggetti; l'ultimo comma di tale articolo si riferisce invece alla necessità di raccordare i criteri di organizzazione delle amministrazioni pubbliche con la legge sulla tutela dei dati personali.

La disciplina dettata da tale disposizione, soprattutto se letta in relazione all'art. 1 (che nel definire il "titolare" ed il "responsabile" prevede, tra coloro che possono rivestire tali qualifiche, anche le pubbliche amministrazioni) e all'art. 2 (che dispone che la legge si applichi al trattamento di dati personali da "chiunque" effettuato nel territorio dello Stato), non individua un regime autonomo e differenziato per il trattamento di dati personali in ambito pubblico.

Il fatto che il trattamento dei dati sia svolto da un soggetto pubblico, anziché da un soggetto privato, non determina, in altre parole, l'applicazione di un regime speciale rispetto a quello stabilito in via generale dalla legge, dato che il pregiudizio che può derivare all'interessato dalla raccolta e dalla circolazione di informazioni inesatte o trattate illecitamente è lo stesso sia che il trattamento avvenga ad opera di un soggetto pubblico, sia che avvenga ad opera di un privato.

Da un certo punto di vista sarebbe addirittura giustificato un rafforzamento degli strumenti di tutela dell'interessato rispetto al trattamento dei dati ad opera della P.A., che, sia sotto il profilo quantitativo, che "autoritativo", può ottenere informazioni difficilmente conseguibili da un privato.

Occorre comunque segnalare che la legge 675/96 non definisce chi sia "soggetto pubblico". Il fatto che l'art. 2 preveda che la legge si applichi ai

trattamenti da "chiunque" effettuati, consente di interpretare estensivamente la nozione di soggetto pubblico: ovvero qualsiasi pubblica amministrazione, ente, associazione, organismo, di natura pubblica. Un'elencazione delle amministrazioni pubbliche è contenuta nell'art. 2 del D.lgs. 3 febbraio 1993, n. 29, che esclude, come la legge 675/96, dal novero delle amministrazioni pubbliche, gli enti pubblici economici.

La legge 675/96 assoggetta dunque gli enti pubblici economici alla disciplina prevista per i privati e questo dato ha fatto sorgere l'interrogativo se, ai fini della 675/96, la distinzione tra soggetti pubblici e privati debba essere basata più che sulla natura giuridica, sul genere di attività effettivamente svolte, con la conseguenza di sottoporre alla disciplina propria dei trattamenti effettuati da soggetti pubblici, quelli svolti da privati per l'esercizio di attività pubbliche (nei limiti di queste).

Anche nell'ambito della pubblica amministrazione, si possono poi individuare le figure del titolare del responsabile e dell'incaricato del trattamento.

La legge 675/96 definisce i criteri per individuare tali soggetti, ma qualora tali criteri si riferiscano a soggetti pubblici è necessario adattarli all'organizzazione amministrativa. Non solo, in alcuni casi sarà la stessa organizzazione amministrativa a dover essere revisionata per consentire la corretta applicazione delle disposizioni della normativa sul trattamento dei dati personali (si veda l'art. 2, quarto comma: "i criteri dell'organizzazione delle amministrazioni pubbliche sono attuati nel pieno rispetto della presente legge").

Segnatamente, in relazione al *titolare*, si tenga presente che esso coincide con l'ente pubblico nel suo complesso, quando allo stesso competono le decisioni in ordine alle finalità e alle modalità del trattamento, ivi compreso il profilo della sicurezza.

Infatti, per titolare si intende il soggetto cui si devono imputare le scelte di fondo, essendo una figura distinta da coloro che sono preposti alle singole operazioni o da colui che è nominato responsabile per i profili operativi, ma che non ha competenza in ordine alle decisioni strategiche.

Quando titolare risulta dunque essere una pubblica amministrazione, per essa operano "nelle diverse scelte che sia necessario assumere, i rispettivi amministratori, secondo le regole che disciplinano ciascuna struttura: di volta in volta, il ministro, l'amministratore delegato, il consiglio di amministrazione, i direttori generali, e gli altri dirigenti ..... Nel caso di grandi enti o amministrazioni, articolati in direzioni generali o in sedi centrali e

periferiche dotate di poteri decisionali del tutto autonomi sui trattamenti effettuati nel loro ambito, le stesse articolazioni possono a loro volta essere considerate come "titolari" o "contitolari" del trattamento"(Comunicato stampa del Garante dell'11 dicembre 1997).

In particolare i compiti del titolare sono:

- individuazione del responsabile (designazione espressa, indicazione analitica dei compiti affidati e specificati per iscritto);
- individuazione per iscritto delle istruzioni al responsabile;
- svolgimento di verifiche periodiche;
- vigilanza sull'osservanza delle disposizioni di legge e delle istruzioni impartite;
- notificazione al Garante.

A garanzia dell'adempimento di tali compiti sono collegate una serie di previsioni sanzionatorie, anche penali, che rendono particolarmente delicata l'individuazione del responsabile, che solitamente è la persona fisica che è al vertice piramidale dell'ente.

Tuttavia la questione non è così semplice: infatti tale figura potrebbe di fatto essere identificata sia in chi ha la rappresentanza dell'ente (Sindaco per il Comune, Rettore per l'università, Ministro per il dicastero o direttori per gli uffici centrali o periferici), sia in chi detiene il potere decisionale, in chi cioè decide effettivamente, ad esempio, laddove sia attuato il D.lgs. 29/93, il direttore generale.

Risulta pertanto auspicabile che ogni soggetto pubblico individui la persona che esprime la volontà dell'ente in ordine al trattamento dei dati o direttamente, con un'indicazione nominativa, o, meglio, indirettamente, facendo riferimento alla carica ricoperta.

Per quanto invece concerne la figura del responsabile (da non confondere con il responsabile del procedimento), si tratta del soggetto preposto al trattamento e la designazione di questo soggetto è facoltativa ed eventuale.

I compiti del responsabile sono:

- procedere al trattamento secondo le istruzioni impartite dal titolare;
- nominare gli incaricati del trattamento.

Il responsabile deve essere nominato tra soggetti che diano garanzia di affidabilità e che siano in grado di assicurare il rispetto della disciplina sul trattamento dei dati anche in ordine ai profili attinenti alla sicurezza. Per quest'ultimo aspetto occorre verificare se la nomina del responsabile è compatibile con la normativa in materia di dirigenza e con il criterio di cui all'art. 10 del D.lgs. 39/93 dell'articolazione omogenea di funzioni e di attività

all'interno degli uffici dell'amministrazione.

La nomina - che deve avere la forma scritta può essere disposta puntualmente per ogni responsabile, oppure può essere prevista con regolamento organizzativo generale, sul modello di quello relativo all'individuazione del responsabile del procedimento amministrativo.

Sarebbe comunque opportuno individuare il responsabile solo dopo aver effettuato una ricognizione delle banche dati gestite dalle varie articolazioni delle pubbliche amministrazioni, anche perché non è escluso che il responsabile del trattamento sia un soggetto esterno all'amministrazione (come, ad esempio, nel caso in cui siano stipulati dalla amministrazione contratti per servizi informatici come l'*outsourcing* o il *disaster recovery*). In quest'ultimo caso la società che tratta i dati è il responsabile del trattamento e la P.A. è il titolare dello stesso.

Gli *incaricati* del trattamento non possono invece essere soggetti terzi ed autonomi dal titolare o dal responsabile, dovendo piuttosto essere subordinati di questi due soggetti.

L'incaricato è la persona fisica che compie materialmente le operazioni relative al trattamento dei dati e che deve elaborare i dati ai quali ha accesso, attenendosi alle istruzioni del titolare o del responsabile. Si noti che la conoscenza dei dati da parte degli incaricati non si considera, ex art. 19 l. 675/96, "comunicazione".

Anche per la nomina dell'incaricato è richiesta la forma scritta e l'individuazione puntuale di mansioni e modalità operative, il che può comportare un appesantimento burocratico dell'organizzazione del lavoro amministrativo.

Una soluzione potrebbe venire, come per molti altri profili della legge, dall'adozione di appositi regolamenti interni, sia che vengano adottati nuovi regolamenti autonomi, espressamente per far fronte alle esigenze organizzative ed operative connesse alle fattispecie relative alla tutela dati personali, sia che vengano aggiornati quelli esistenti, ad esempio quelli disciplinanti il diritto di accesso ai documenti (come già ad esempio hanno fatto molti enti locali).

In ordine al trattamento effettuato da soggetti pubblici, sebbene, come accennato, la disciplina della legge 675/96 non preveda un regime speciale, esistono tuttavia alcune differenziazioni rispetto al trattamento ad opera di privati: l'informativa da rendere all'interessato al momento della raccolta ha un contenuto più limitato (ai sensi dell'art. 10, seconda comma); non è necessario il consenso espresso dell'interessato per poter procedere al

trattamento (art. 11); l'esercizio di alcuni dei diritti di cui all'art. 13 da parte dell'interessato può subire limitazioni rispetto ai trattamenti effettuati da soggetti pubblici in base ad espressa disposizione di legge e per le finalità indicate dalla legge (art. 14, primo comma, lettera d); il trattamento dei "dati sensibili" da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge che ne disciplini limiti e finalità (art. 22, terzo comma); norme particolari sono dettate per il trattamento di dati inerenti alla salute trattati da organismi pubblici (art. 23).

## **10. (segue) La normativa sul trattamento dei dati personali**

L'attività rispetto alla quale la diversità di disciplina tra i trattamenti effettuati da soggetti pubblici e privati è più significativa (almeno ai nostri fini), è quella, più volte richiamata, di comunicazione e di diffusione di dati: l'art. 20, infatti, dispone solo in ordine al caso che tali operazioni siano svolte da soggetti privati (o enti pubblici economici, sempre equiparati ai privati), rinviando, per la disciplina di tali attività poste in essere da soggetti pubblici, all'art. 27.

L'art. 27 indica le condizioni che legittimano i soggetti pubblici al trattamento dei dati e che sono individuate mediante rinvio a "leggi e regolamenti".

In primo luogo il trattamento è consentito soltanto per lo svolgimento delle finalità istituzionali del soggetto pubblico, in altre parole una amministrazione non può gestire una banca dati per scopi diversi dalle funzioni che le sono proprie, ma non è certo agevole, sul piano dei fatti, individuare in concreto, tra gli innumerevoli dati comunicati dai privati ai soggetti pubblici, se alcuni esulino o eccedano rispetto allo svolgimento delle funzioni istituzionali.

Si tenga inoltre presente che l'ingente mole di informazioni trattate dalla P.A. - come dimostra il lavoro svolto - sono raccolte in forza di disposizioni normative ormai datate, dettate in un momento in cui la comunicazione di dati da parte del privato all'amministrazione veniva considerata come una sorta di obbligazione (solo talvolta bilanciata dal fatto di essere strumentale ad ottenere una prestazione) e la raccolta di dati da parte della pubblica amministrazione veniva semplicemente inquadrata nell'ambito del tradizionale principio di legalità dell'azione amministrativa.

Occorre, in altre parole, tenere conto del fatto che l'informatizzazione della P.A., se da un lato ha semplificato l'azione amministrativa, dall'altro ha

accresciuto le possibilità di accesso alle informazioni in possesso della P.A., la quale le ha raccolte o se ne è trovata in possesso, in forza di disposizioni scritte da un legislatore ancora noncurante del problema dei limiti entro i quali tali dati potevano essere utilizzati.

In ordine alle modalità di comunicazione ("il dare conoscenza dei dati personali ad uno o più soggetti determinati, diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione") e di diffusione ("il dare conoscenza dei dati a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione") di dati personali da parte dei soggetti pubblici, la disciplina è data, come abbiamo detto, dal secondo e terzo comma dell'art. 27, a seconda che destinatario sia un soggetto pubblico o privato.

Nel primo caso, è necessario che tale operazione sia prevista da norme di legge o di regolamento oppure che sia necessaria allo svolgimento delle funzioni istituzionali; in tal caso è richiesta però una preventiva comunicazione al Garante, che può eventualmente vietare la comunicazione o la diffusione.

In tale contesto viene anche in considerazione il problema del trasferimento di dati da un'amministrazione all'altra, che è processo fortemente incentivato dalle leggi che negli ultimi anni tentano di rendere più efficiente l'organizzazione ed i procedimenti amministrativi.

Tra le disposizioni di legge che prevedono lo scambio tra amministrazioni di dati a carattere personale possiamo citare, a mero titolo esemplificativo, l'articolo unico del D.P.R. 31 dicembre 1971, n. 1388, in materia di trasmissione di dati tra gli enti erogatori di pensione ed il casellario centrale dei pensionati; il D.lgs. 12 luglio 1991, n. 212, che consente alle pubbliche amministrazioni e ad altri soggetti pubblici l'accesso al sistema informativo dell'anagrafe tributaria; alla legge 7 dicembre 1989, n. 389, che all'art. 4, VII comma, prevede il reciproco accesso diretto di INPS ed INAIL agli archivi delle Camere di commercio e di quelli collegati al registro delle imprese.

Venendo infine all'ipotesi di comunicazione o diffusione di dati personali ad un privato da parte di un soggetto pubblico, l'art. 27, terzo comma, della legge 675/96, consente tali operazioni solo se espressamente previste da norme di legge o di regolamento.

Sembrirebbe di dovere interpretare restrittivamente il citato disposto, nel senso che, solo in presenza di una specifica disposizione normativa, un soggetto pubblico possa dare conoscenza a terzi dei dati personali, dallo stesso detenuti.

E' evidente, però, che tale disposizione deve essere armonizzata con

quanto previsto dalla normativa sul diritto di accesso agli atti amministrativi.

La legge 675/96 non dice come contemperare le opposte esigenze di trasparenza dell'attività amministrativa e di esercizio del diritto di accesso dei cittadini ai documenti amministrativi (sanciti dalla legge n. 241/90), con quelle di tutela dei diritti dei singoli rispetto al trattamento dei dati personali ad opera delle pubbliche amministrazioni (salvaguardate appunto dalla legge 675/96).

Conseguentemente il problema maggiore resta quello di individuare le modalità con cui in concreto le amministrazioni che trattano dati devono procedere per realizzare il contemperamento di tali contrapposti interessi.

## **11. I problemi ancora aperti**

Nonostante il quadro normativo e giurisprudenziale sopra descritto, i problemi che l'operatore pubblico si trova ad affrontare all'atto pratico sono ancora tutti aperti, trattandosi in buona sostanza di individuare la disciplina di riferimento del suo agire, di comprendere se il rilascio di un'informazione ai sensi della legge sull'accesso agli atti amministrativi sia o meno in contrasto con la disciplina sul trattamento dei dati personali. Con l'evidente rischio, in mancanza di chiarezza, di rallentare il processo di semplificazione e informatizzazione amministrativa.

Si pensi all'ipotesi che venga richiesto al dipendente comunale - nelle amministrazioni locali, come visto, il problema è più urgente, sia per l'estensione del diritto di accesso così come previsto dall'art. 7 della legge 142/90, sia per il frequente contatto dell'amministrazione con l'utente - se il Sindaco ha rilasciato a un determinato soggetto un certificato di buona condotta, oppure se sono stati concessi contributi ai sensi della legge n. 13/89 per l'eliminazione delle barriere architettoniche o se è stato avviato un procedimento che riguarda un terzo.

In tali casi e in molti altri ancora, l'accesso al documento lede la riservatezza di uno o più terzi, cosicché sembrerebbe opportuno che le amministrazioni adottino delle direttive guida rivolte sia all'operatore che all'utente che, standardizzando i vari casi, forniscano i criteri di prevalenza tra le diverse esigenze.

A mero titolo di esempio, a fronte della richiesta di accesso finalizzata alla cura e tutela dei propri interessi giuridici, l'amministrazione potrebbe chiedere che venga fornita una prova anche non formale di tale interesse; oppure potrebbe essere ipotizzata una comunicazione al soggetto la cui

privacy potrebbe risultare violata dall'accesso perché intervenga con proprie controdeduzioni alla richiesta di accesso; o ancora potrebbero essere previsti i casi in cui l'accesso è garantito ma previa criptazione delle parti del documento che potrebbero compromettere la riservatezza, soluzione questa certo da suggerire in via prospettiva di evoluzione ed informatizzazione della P.A..

Inoltre, anche per le ipotesi di dati che la P.A. può comunicare sicuramente ai richiedenti in quanto questa circostanza è prevista da norme di legge, o regolamento (ad esempio i dati inseriti in pubblici registri che, in quanto tali, sono consultabili e accessibili da parte di chiunque) l'amministrazione è comunque tenuta a osservare alcune cautele non solo per quanto riguarda la citata comunicazione e diffusione dei dati dopo l'entrata in vigore della legge n. 675, ma anche per quanto riguarda la disciplina generale sul trattamento: come visto, sul piano concreto si pone il problema dell'individuazione del titolare e del responsabile del trattamento, nonché dell'adozione delle misure di sicurezza o della previsione di elaborazione di trattamenti automatizzati ex art. 17 della legge n. 675/96.

Un altro problema di non poco momento che l'entrata in vigore della legge n. 675 pone agli enti pubblici è infatti quello organizzativo, vale a dire quale sia l'ufficio che debba occuparsi dell'applicazione della legge, e come conciliare tali previsioni con quelle, parimenti organizzative, delle leggi nn. 142 e 241.

Alcuni ministeri, per esempio, hanno optato per designare come centro di responsabilità l'ufficio per i sistemi informativi automatizzati (così ad esempio il Ministero del lavoro), fermo restando che la legge riguarda anche le banche dati su supporti cartacei, delle quali spesso è stato necessario fare una ricognizione.

Da qui discende la necessità di accertare la realtà esistente e fornire soluzioni uniformi per i vari "addetti" al trattamento dei dati.

E' quantomai auspicabile, pertanto, che almeno gli enti locali, nell'attesa che venga approntata una disciplina organica della gestione delle informazioni in possesso della P.A., regolamentino unitariamente la gestione delle informazioni in loro possesso, elaborando regolamenti o linee guida a vantaggio sia dei dipendenti pubblici che dei cittadini.

## 12. Il lavoro svolto

Alla luce di tutto ciò diviene urgente prima di tutto chiarire quanto più possibile - e, *per incidens*, non è fino in fondo possibile - i dati che una P.A. si trova a trattare, quindi le banche dati di sua gestione o quelle a cui è interconnessa, in definitiva il suo potere informatico.

Da qui l'esigenza - a cui questo lavoro cerca di far fronte - di "ordinare" la normativa, spesso stratificata, che regola la tenuta di archivi, individuando la legge originaria, le eventuali disposizioni sopravvenute e tutte le norme dettate nella fase di informatizzazione degli archivi pubblici.

Chiarire infatti come funziona una banca dati, le finalità a cui è preordinata, le eventuali cautele a cui è sottoposta e gli accessi consentiti appare di fondamentale importanza per verificare le sue potenzialità lesive in rapporto all'esigenza di riservatezza.

La ricerca compiuta fin qui si è svolta su basi fondamentalmente empiriche, nella convinzione che per "risolvere" concretamente i problemi dell'operatore pubblico in materia, si debba partire dal dato di fatto, quindi dal dato normativo che questi deve in definitiva applicare.

Proprio a tal proposito occorre però specificare, quale caveat, che la ricerca effettuata non ha né può avere pretese di completezza: come già accennato, la normativa in materia che tratta o concerne, direttamente e indirettamente, delle banche dati delle Pubbliche Amministrazioni è, come anche risulta dal lavoro svolto, disseminata nei più vari testi normativi, vari sia per oggetto, essendo profondamente eterogenei i provvedimenti che contengono riferimenti a banche dati (si pensi alla banca dati per il registro del sangue o a quella per la rilevazione della tubercolosi negli allevamenti bovini e bufalini), sia per natura, trattandosi di leggi, decreti del Presidente della Repubblica, decreti legislativi, decreti ministeriali, decreti del Presidente del Consiglio dei ministri, ordinanze ministeriali, e via dicendo.

Vi è poi da considerare che, oltre ai dati che il soggetto pubblico è tenuto per legge a trattare, vi sono anche quelli posseduti occasionalmente.

Infine, alla difficoltà di far fronte a questa mole di norme, occorre ricordare che di informatizzazione trattano anche le leggi regionali - che nel presente rapporto sono state analizzate solo per la Regione Toscana - nonché tutti i regolamenti regionali e locali che si trovano ad affrontare nel dettaglio i problemi sollevati in concreto da questa fase essenziale dell'agire amministrativo.

Da tutto ciò emerge con particolare evidenza la trasversalità della materia

in oggetto e anche la sua strumentalità, tanto da poterla qualificare come una modalità dell'azione amministrativa.

### **13. La metodologia seguita**

Quanto alla metodologia seguita, si è ritenuto opportuno tenere distinta la normativa che concerne lo Stato e i soggetti pubblici statali, da quella relativa alle regioni e agli enti locali, riportando in entrambi i gruppi quelle normative che abbiano a oggetto una banca dati statale con articolazioni periferiche o viceversa (banche dati regionali o locali che siano interconnesse con organi centrali).

Occorre inoltre dar conto dei criteri adottati per le catalogazioni della normativa rintracciata: si è scelto di tenere conto dello "sforzo" del legislatore in materia di informatizzazione, ovvero cosa e quanto viene previsto quando si istituisce o si fa riferimento a banche dati o sistemi informativi.

Questo criterio è infatti sembrato quello che meglio mette in luce il peso dell'attenzione dedicata dal legislatore e quindi, in definitiva, l'importanza che, in misura sempre crescente negli anni, tale materia ha assunto nel nostro ordinamento.

Un altro criterio che potrebbe essere seguito è quello di distinguere le normative a seconda del soggetto gestore della banca dati. In tal caso si potrebbero individuare tre grandi gruppi facenti capo all'Amministrazione statale (segnatamente le banche dati ministeriali), ai soggetti pubblici statali operanti su tutto il territorio nazionale (per esempio le banche dati delle Camere di Commercio, dell'Eima, delle Amministrazioni autonome dei monopoli di Stato, ecc.) e infine alle regioni ed enti locali.

L'opzione finale è stata di adottare il criterio "contenutistico" tenendo distinte, come detto, le normative in due grandi gruppi, banche dati statali, da una parte, regionali e locali, dall'altra, soddisfacendo in parte anche il criterio "soggettivistico".

In tal modo si sono potute apprezzare anche le differenze tra apparato statale e apparato periferico, o meglio, le omogeneità, dal momento che si è potuta riscontrare una sostanziale corrispondenza nella previsione di informatizzazione, così da poter essere in definitiva stimolata l'interconnessione.

Sono state infine tenute distinte quelle normative che costituivano per la loro affinità un raggruppamento a parte, come quelle concernenti le Camere

di Commercio o quella relativa alla rete unitaria della P.A.. Infine sono state distinte anche le normative istitutive o facenti riferimento a banche dati di derivazione comunitaria.

#### **14. I primi risultati**

La disponibilità di questi dati normativi così ordinati ha consentito l'elaborazione di un quadro tipo sinottico in cui poter inserire le singole banche dati.

Tale scheda mette in rilievo gli aspetti più significativi delle banche dati così da esserne immediatamente percepibile la natura e il funzionamento.

In primo luogo si dà conto della legge istitutiva e delle eventuali leggi o regolamenti a disciplina: ciò permette innanzitutto di vedere storicamente quando si concentrano i provvedimenti di istituzione delle banche dati (negli anni '90, principalmente) così da valutarne la sensibilità o meno ai problemi di accesso e di riservatezza.

In seconda battuta sono evidenziate le finalità per cui viene istituita la banca dati, elemento che può essere valutato per chiarire il rapporto con la riservatezza.

Segue l'individuazione del soggetto gestore, delle eventuali articolazioni periferiche, delle modalità di informatizzazione (se direttamente o tramite affidamento a terzi), dei soggetti obbligati o facoltizzati a fornire i dati, dei soggetti che possono accedere e delle modalità dell'accesso. E' poi specificato il collegamento con altre banche dati (interconnessione), l'eventuale previsione di specifici divieti di accesso, le sanzioni per il mancato scambio dei dati e infine la previsione delle garanzie per la riservatezza.

A titolo esemplificativo sono state prese in considerazione le banche dati del S.I.L. (Sistema Informativo Lavoro) e dell'anagrafe civile, scelte in considerazione del fatto che sono tra quelle più dettagliatamente disciplinate; pur essendo anche queste, come, del resto, tutte le banche dati analizzate, prive di una specifica regolamentazione in ordine al temperamento tra esigenze di riservatezza e di sicurezza e quelle di accesso.

L'utilizzazione della scheda può essere inoltre un punto di partenza per effettuare una tipizzazione delle banche dati gestite da pubbliche amministrazioni. Possono essere distinte, ad esempio, a seconda della più o meno marcata connotazione "commerciale", come si desume dal fatto che l'accesso sia o meno a titolo oneroso, che le modalità di

## BANCA DATI

Legge istitutiva di derivazione comunitaria	11
Leggi e regolamenti a disciplina	
Finalità	
Soggetto gestore della b.d.	
Articolazioni periferiche	
Modalità dell'informatizzazione	
Affidamento a terzi in concessione	
Soggetti che forniscono i dati	
come obbligo	
come facoltà	
Responsabile del procedimento	
Procede all'interrogazione dell'archivio	
Responsabile della sicurezza	
Soggetti che possono accedere	
A titolo gratuito	
A titolo oneroso	
Una persona individuata	
L'ente in generale	
A tutta la bancadati	
Ad alcuni dati	
Al documento	
A scopo informativo	
A scopo professionale	

*segue* BANCA DATI

Collegamento con altre banche dati (interconnessione)	
Come obbligo	
Come facoltà	
Modalità di interconness.	
Specifici divieti di accesso	
Ai dati	
Al documento	
Sanzioni per non aver fornito o scambiato dati	
Garanzie della riservatezza ex l. 675/96	
Adeguamento in via interpretativa	
Esonero dall'applicazione della 675	

## BANCA DATI: S.I.L. (*Sistema informativo lavoro*)

Legge istitutiva di derivazione comunitaria	D.lgs. 23 dicembre 1997, n. 469 I I
Leggi e regolamenti a disciplina	NO
Finalità	Risponde alle finalità e ai criteri stabiliti dall'art. 1 del D.lgs. 12.2.1993, n. 39 (Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche)
Soggetto gestore della b.d.	Ministero del lavoro e della previdenza sociale
Articolazioni periferiche	<i>Regioni e enti locali possono provvedere allo sviluppo autonomo di parti del sistema</i>
Modalità dell'informatizzazione	<i>"Si avvale dei servizi di interoperabilità e delle architetture di cooperazione previste dal progetto di rete unitaria della P.A." (art. 11, III co.)</i>
Affidamento a terzi in concessione	
Soggetti che forniscono i dati	<i>Min. lavoro; regioni; enti locali; soggetti autorizzati alla mediazione tra domanda e offerta di lavoro.</i>
come obbligo	<b>SI ("obbligo di connessione e scambio dei dati")</b>
come facoltà	
Responsabile del procedimento	NO
Procede all'interrogazione dell'archivio	
Responsabile della sicurezza	NO
Soggetti che possono accedere	<i>Le imprese di fornitura di lavoro temporaneo e i soggetti autorizzati alla mediaz. tra dom e off. di lav. Tramite convenzione con il Ministero</i>
A titolo gratuito	
A titolo oneroso	<b>SI secondo tariffe determinate dal Min. sentita l'AIPA</b>
Una persona individuata	
L'ente in generale	<b>SI</b>
A tutta la bancadati	<b>SI</b>
Ad alcuni dati	
Al documento	
A scopo informativo	
A scopo professionale	

segue BANCA DATI: S.I.L. (*Sistema informativo lavoro*)

Collegamento con altre banche dati (interconnessione)	<i>E' prevista la piena trasparenza alle anagrafi e lo scambio dei dati ("servizio di scambio telematico di dati tra Comuni e gli organismi" interessati)</i>
Come obbligo	
Come facoltà	
Modalità di interconness.	
Specifici divieti di accesso	<b>NO</b>
Ai dati	
Al documento	
Sanzioni per non aver fornito o scambiato dati	<i>Il mancato scambio delle infor. e dei dati comporta la sospensione dall'incarico disposta con decr. Del Min. vigilante, per un periodo di sei mesi, dei leg. Rappr. degli enti di cui sopra o dei dirigenti specificamente preposti (art. 2, 7 co., l. 63/93)</i>
Garanzie della riservatezza ex l. 675/96	<i>Ai fini della sicurezza, i comuni e i soggetti di cui supra regolamentano l'accesso ai dati, sulla base di criteri di autorizzazione, attraverso idonee procedure informatiche atte ad identificare e registrare gli operatori a terminale e le operazioni effettuate. (art. 7 D.P.R. 5 maggio 94)</i>
Adeguamento in via interpretativa	
Esonero dall'applicazione della 675	

## BANCA DATI: ANAGRAFE DELLO STATO CIVILE (codice fiscale)

Legge istitutiva Di derivazione comunitaria	D.P.R. 2 novembre 1976, n. 784 <i>Legge 17 marzo 1993, n. 63</i> I I
Leggi e regolamenti a disciplina	D.P.R. 5 maggio 1994
Finalità	consentire l'acquisizione del codice fiscale, quale elemento identificativo di ogni soggetto, tra P.A. e tra queste e organismi che esercitano attività di prelievo contributivo e fiscale, che erogano servizi di pubblica utilità o preposti all'informazione statistica pubblica .
Soggetto gestore della b.d.	<b>Ministero delle finanze (genera il codice fiscale sulla base dei dati forniti)</b>
Articolazioni periferiche	<b>Comuni</b>
Modalità dell'informatizzazione	<i>Le PP.AA. centrali e locali nonché i soggetti privati interessati dalla presente b.d. (vd. infra) utilizzano le reti pubbliche di trasmissione dati ovvero le reti private dei soggetti interessati, purché conformi agli standard usati nelle reti pubbliche. I comuni possono utilizzare la rete dell'ANCI</i>
Affidamento a terzi in concessione	
Soggetti che forniscono i dati	<i>Comuni; organismi che esercitano attività di prelievo contributivo e fiscale, che erogano servizi di pubblica utilità o preposti all'informazione statistica pubblica</i>
come obbligo	
come facoltà	
Responsabile del procedimento	<b>"Responsabile dei collegamenti che autorizza i soggetti che hanno accesso ai dati" designato dai comuni e dagli organismi privati ( art. 8 D.P.R. 5 maggio 1994)</b>
Procede all'interrogazione dell'archivio	
Responsabile della sicurezza	
Soggetti che possono accedere	<b>Gli stessi che forniscono i dati</b>
A titolo gratuito	<b>SI</b>
A titolo oneroso	
Una persona individuata	
L'ente in generale	<b>SI</b>
A tutta la bancadati	

## segue BANCA DATI: ANAGRAFE DELLO STATO CIVILE (codice fiscale)

Ad alcuni dati	<i>Ai dati funzionali alle esigenze istituzionali del richiedente, definiti con provvedimento dei soggetti interessati</i>
Al documento	
A scopo informativo	
A scopo professionale	<b>SI</b>
Collegamento con altre banche dati (interconnessione)	<i>E' prevista la piena trasparenza alle anagrafi e lo scambio dei dati ("servizio di scambio telematico di dati tra Comuni e gli organismi" interessati)</i>
Come obbligo	
Come facoltà	
Modalità di interconness.	
Specifici divieti di accesso	<b>NO</b>
Ai dati	
Al documento	
Sanzioni per non aver fornito o scambiato dati	<i>Il mancato scambio delle infor. e dei dati comporta la sospensione dall'incarico disposta con decr. Del Min. vigilante, per un periodo di sei mesi, dei leg. Rapp. degli enti di cui sopra o dei dirigenti specificamente preposti (art. 2, 7 co., l. 63/93)</i>
Garanzie della riservatezza ex l. 675/96	<i>Ai fini della sicurezza, i comuni e i soggetti di cui supra regolamentano l'accesso ai dati, sulla base di criteri di autorizzazione, attraverso idonee procedure informatiche atte ad identificare e registrare gli operatori a terminale e le operazioni effettuate. (art. 7 D.P.R. 5 maggio 94)</i>
Adeguamento in via interpretativa	
Esonero dall'applicazione della 675	

interconnessione possano o meno avvenire mediante convenzioni anche a titolo oneroso o, infine, dalla tipologia dei soggetti che hanno interesse ad accedere alla banca dati. Caratteristiche di tipo "commerciale" si riscontrano ad esempio nel S.I.L., a fronte di quanto è invece disposto per l'anagrafe civile, per la quale l'accesso è a titolo gratuito e sono previste sanzioni per la mancata fornitura o scambio di dati.

Questi ed altri confronti, resi di immediata evidenza dall'utilizzazione della scheda, ci auspichiamo che facciano emergere gli aspetti più problematici e possano rendere più agevole il compito dell'interprete.

## GLOSSARIO

**ATTIVITÀ AMMINISTRATIVA** (alla quale è correlato il diritto di accesso): attività di diritto amministrativo e attività di diritto privato volta alla cura concreta di interessi della collettività (Cons. Stato, sez. IV, 15.01.1998, n. 14)

**BANCA DATI**: qualsiasi complesso di dati personali, ripartito in una o più unità dislocate in uno o più siti, organizzato secondo una pluralità di criteri determinati tali da facilitarne il trattamento

**COMUNICAZIONE**: dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione

**DATI PERSONALI**: qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, compresi numeri di identificazione personale

**DATI SENSIBILI**: dati personali idonei a rilevare l'origine razziale, le convinzioni religiose, lo stato di salute e la vita sessuale

**DIFFUSIONE**: dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione

**DIRITTO DI ACCESSO**: visione ed estrazione di copia di documenti amministrativi; diritto soggettivo all'informazione

**DISSEMINATION**: dovere della Pubblica Amministrazione di informazione, per favorire la conoscenza dei cittadini su atti, documenti e in genere dati in possesso della P.A.

**DOCUMENTO AMMINISTRATIVO**: ogni rappresentazione grafica, fotocinematografica, elettromagnetica, o di qualunque altra specie, che contenga gli atti della Pubblica amministrazione (l. 241/90)

**GARANTE:** organo collegiale, composto da quattro membri, eletti tra persone di particolare competenza professionale, con carica quadriennale, piena autonomia e indipendenza di giudizio e valutazione

**INCARICATO DEL TRATTAMENTO:** colui il quale deve elaborare i dati personali a cui ha accesso, attenendosi alle istruzioni del titolare o del responsabile

**INFORMAZIONE:** qualunque elemento idoneo a creare conoscenza circa fatti, situazioni o stati riguardanti il soggetto stesso

**INTERCONNESSIONE:** collegamento tra banche dati

**RESPONSABILE:** soggetto preposto dalla Pubblica Amministrazione al trattamento dei dati personali

**RISERVATEZZA:** libertà da intrusioni della curiosità sociale, delle comunicazioni sociali, del potere pubblico

**TITOLARE:** l'ente a cui competono le decisioni in ordine alle finalità e alle modalità di trattamento di dati personali, ivi compreso il profilo della sicurezza (l. 675/96)

**TRATTAMENTO:** qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, 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 dei dati

## PARTE SECONDA

### BANCHE DATI E TUTELA DELLA PRIVACY NELLE PUBBLICHE AMMINISTRAZIONI: PROFILI TECNICI ED ESPERIENZE PRATICHE

1. Premessa al lavoro svolto - 2. I termini del problema - 3. Gli standard internazionali sulla sicurezza informatica - 4. Lo standard ITSEC - 4.1. *La struttura dello standard ITSEC* - 4.2 *L'obiettivo di sicurezza* - 4.3. *La valutazione dell'efficacia* - 4.4. *La valutazione della correttezza* - 5. L'uso dello standard ITSEC nella P.A. - 6. I problemi ancora aperti.

#### **1. Premessa al lavoro svolto**

Nelle parte prima di questo documento sono stati esaminati i problemi giuridici relativamente all'apparente conflitto fra la riservatezza e l'accesso, così come essi emergono dalla normativa vigente. In questa seconda parte si intendono invece esaminare i problemi di carattere tecnologico che le normative pongono nel momento in cui si deve dare ad esse concreta attuazione. L'attenzione è rivolta in particolare alla sicurezza di sistemi automatici per il trattamento delle informazioni, ossia alla sicurezza informatica, intendendo come sicurezza la combinazione di tre attributi:

- **riservatezza**: solo le persone autorizzate hanno accesso alle informazioni contenute nel sistema informatico;

- **integrità**: le informazioni non possono essere alterate in modo arbitrario da chiunque;
- **disponibilità**: le informazioni sono disponibili alle persone autorizzate nei tempi e nei modi previsti.

L'obiettivo è creare un quadro di riferimento delle opzioni tecnologiche sia per il legislatore che per i responsabili informatici delle PPAA., al fine di identificare quali sono le "sicurezze" effettivamente realizzabili e contemporaneamente quali sono le "sicurezze" da realizzare.

Il punto di partenza è che tutte le PPAA., come già evidenziato, devono raccogliere informazioni che rientrano nell'ambito di applicazione della legge n. 675/1996, sia per la gestione quotidiana del loro lavoro, sia perché sono obbligate da leggi dello Stato. In ogni caso oggi e ancor più domani saranno presenti all'interno delle PPAA. informazioni riguardanti persone fisiche o giuridiche - in breve, dati soggetti alla legge n. 675/1996.

Le normative sull'accesso ai dati e la progressiva diffusione dell'informatizzazione all'interno della P.A. premono contemporaneamente per semplificare l'accesso da parte dei cittadini e di altre amministrazioni a queste informazioni. Pertanto, le basi dati che si vengono a costituire non sono strutture isolate e quindi facilmente controllabili. Sono al contrario immerse in sistemi complessi (quali ad esempio la P.U.P.A.), in cui non è possibile a priori stabilire chi sono i soggetti che effettueranno l'accesso.

D'altro canto, la natura dei dati contenuti in questi archivi informatici impone necessariamente il loro controllo secondo la legge n. 675/1996, il cui recente regolamento di attuazione (le cosiddette misure di sicurezza minime) rappresenta una prima indicazione delle misure da adottare, in base alla tipologia di informazioni trattate. Tali indicazioni sono tuttavia, dal punto di vista tecnologico, insufficienti per la creazione di sistemi sicuri.

Le misure proposte pongono infatti l'accento sull'uso di provvedimenti organizzativi e misure di sicurezza tecnologiche per la sicurezza dei sistemi informatici. Mentre è assolutamente corretto utilizzare provvedimenti organizzativi per garantire la sicurezza di un sistema informatico, un insieme di misure di sicurezza tecnologiche prive di un adeguato livello di affidabilità rischiano di essere un inutile appesantimento del sistema stesso.

Per dettagliare meglio questa affermazione paradossale, è utile ricordare

che dal punto di vista informatico la sicurezza è una proprietà negativa: è banale dimostrare che un sistema non la possiede, ma è impossibile dimostrare che un sistema la possiede. Ad esempio, se a causa di un errore di configurazione è possibile accedere a un sistema senza inserire una parola chiave di riconoscimento, il sistema è ovviamente non sicuro. Analogamente, se all'interno di un sistema è presente un programma "cavallo di Troia" (ossia, un programma che consente un accesso mascherato e illecito all'intero sistema) il sistema è ancora non sicuro.

D'altro canto, dimostrare che un sistema è sicuro è un problema radicalmente differente. Esso richiede di esaminare tutto il sistema alla ricerca di vulnerabilità note. Tuttavia, la loro assenza non permette di decidere che il sistema non presenta ulteriori vulnerabilità: la recente storia informatica ci ha anzi dimostrato che i sistemi rivelano nuove vulnerabilità nel tempo.

## 2. I termini del problema

Se quindi la sicurezza è una proprietà negativa, che non può essere valutata, è necessario fare riferimento ad altre caratteristiche dei sistemi informatici, che rispondano a esigenze diverse da parte dei soggetti coinvolti. In particolare:

- devono garantire ai cittadini che i dati in possesso della P.A. siano trattati con le cure dovute;
- devono fornire alla singola amministrazione uno strumento per definire i requisiti dei propri sistemi informativi, e per valutare l'efficacia (in termini di sicurezza) di quelli esistenti;
- devono fornire alle autorità preposte al controllo (quali il garante della Privacy) uno strumento per verificare in modo uniforme e imparziale l'adeguatezza delle misure prese con il dettaglio delle norme giuridiche.

L'impossibilità di misurare direttamente la sicurezza di un sistema informatico è stata verificata con mezzi empirici. In particolare, sono stati impiegati gruppi di esperti che hanno aggredito uno stesso sistema alla ricerca di potenziali vulnerabilità. Il risultato di tali esperimenti è stato che gruppi diversi hanno identificato vulnerabilità diverse, tipicamente in base al background culturale di ciascun membro di un gruppo. Pertanto, se un gruppo poteva non identificare alcuna vulnerabilità e quindi considerare un sistema sicuro, un gruppo diverso poteva identificarne più di una sullo stesso sistema.

Da quanto esposto sopra, risulta chiaro perché nel mondo informatico il concetto di valutazione diretta della sicurezza di un sistema è stato abbandonato in favore del concetto di valutazione del processo di creazione della sicurezza. Tale valutazione è simile come concetto alla certificazione della qualità, in cui si valuta il processo anziché il prodotto finito. Si parla pertanto di sistemi credibili (trusted), poiché attraverso un processo di valutazione l'utente finale acquisisce fiducia che il sistema sia in grado di soddisfare le proprie esigenze di sicurezza. Il livello di fiducia è collegato alla profondità del processo di valutazione e viene denominata affidabilità (assurance).

Un punto importante riguardo i sistemi trusted è che essi inevitabilmente offrono garanzie (ossia limitano i rischi di violazione della sicurezza) solo fino a un certo punto. Non esiste infatti nessuna garanzia assoluta che un sistema trusted non sia violato. In generale, come regola empirica, al decrescere del rischio di violazione cresce il costo del sistema trusted, poiché in generale il processo di esame del sistema è stato più complesso e articolato, e ha richiesto maggiori risorse.

Quest'ultimo punto sottolinea un'ulteriore carenza delle normative attuali, ossia quello relativo ai costi di adeguamento dei sistemi agli standard di sicurezza, e contemporaneamente la garanzia per la P.A. che tali adeguamenti siano sufficienti a rispondere ai requisiti della legge. Non è infatti pensabile che la P.A. disponga di risorse economiche illimitate per garantire la sicurezza delle informazioni in proprio possesso, o che sia lasciato all'arbitrio delle singole PPA.A. quale livello di sicurezza scegliere per i propri sistemi.

Infatti, come vedremo in seguito, l'esistenza di una specifica misura di sicurezza in sistemi diversi (p.e., un accesso controllato tramite parola chiave) è assolutamente non confrontabile se non si può avere una valutazione della credibilità di tale misura di sicurezza.

### **3. Gli standard internazionali sulla sicurezza informatica**

Al fine di consentire la possibilità di valutare la credibilità dei sistemi informatici, sono stati sviluppati in ambito nazionale ed internazionale alcuni standard per la valutazione della sicurezza dei sistemi. In questo momento i due principali standard di riferimento per l'Europa sono lo standard ITSEC (Information Technology Security Evaluation Criteria, Criteri per la Valutazione della Sicurezza della Tecnologia Informatica), sviluppato dalla

Comunità Europea ed adottato da Francia, Gran Bretagna e Germania e lo standard CC (Common Criteria, Criteri Comuni), sviluppato dai paesi che hanno adottato ITSEC in collaborazione con Canada e Stati Uniti.

In questo documento si è preferito dare maggiore risalto allo standard ITSEC, poiché esso è ben compreso e ormai diffuso. Lo standard CC è di recentissima definizione e comunque è per definizione compatibile con lo standard ITSEC.

#### **4. Lo standard ITSEC**

Di seguito è riportata una presentazione in dettaglio dello standard ITSEC. La presentazione segue l'organizzazione dei contenuti così come è presente all'interno del documento ufficiale dello standard. Con questa presentazione non si vuole fare una semplice esposizione di ITSEC, quanto piuttosto mostrare come esso possa essere adattato (e quindi adottato) per consentire al legislatore di fornire norme stringenti e allo stesso tempo per dare spazio a una valutazione semplice e imparziale della loro applicazione.

##### *4.1 La struttura dello standard ITSEC*

In ITSEC, sono identificati:

- un sistema da valutare denominato Oggetto di Valutazione (Target of Evaluation, TOE);
- un insieme di requisiti di sicurezza, denominati Obiettivo di Sicurezza (Security Target, ST);
- uno sponsor della valutazione del sistema;
- un ente di valutazione del sistema.

Lo sponsor propone a un ente di valutazione un determinato sistema, richiedendo che l'ente verifichi che esso risponde agli obiettivi di sicurezza che sono stati specificati. ITSEC fornisce uno schema di riferimento per quello che riguarda la specifica dei requisiti di sicurezza, al fine di consentirne la valutazione. Nel seguito essi saranno ulteriormente descritti.

Si può tuttavia già notare il collegamento esistente fra lo schema identificato e i requisiti minimi di sicurezza per la privacy. E' infatti possibile

identificare con gli Oggetti di Valutazione i sistemi informatici per il trattamento dei dati personali; con gli sponsor le P.P.A.A. interessate a verificare la rispondenza dei propri sistemi ai requisiti di sicurezza imposti dalla legge; e infine con l'ente di valutazione lo stesso Garante della Privacy o enti da esso accreditati per effettuare la valutazione dei sistemi.

#### *4.2. L'obiettivo di sicurezza*

L'obiettivo di sicurezza è un documento che specifica l'ambiente in cui un sistema deve operare e le misure di sicurezza che esso adotta contro le minacce presenti nel suo ambiente.

Un obiettivo di sicurezza è composto di quattro parti:

- La Politica di Sicurezza di Sistema;
- La specifica delle funzioni di sicurezza richieste;
- La loro efficacia in termini di resistenza a un attacco diretto;
- Il livello di esame della correttezza della loro implementazione.

La **Politica di Sicurezza di Sistema** identifica le minacce al sistema informatico, gli obiettivi di riduzione delle minacce e l'insieme di leggi, regolamenti e prassi che regolano il trattamento delle informazioni al suo interno. Lo scopo di una politica di sicurezza non è definire gli strumenti per la gestione della sicurezza, quanto identificare le priorità e giustificarle.

Le **Funzioni di Sicurezza** identificano che cosa l'Oggetto di Valutazione garantisce ai propri utenti in termini di sicurezza. Lo standard non impone alcuna funzione di sicurezza specifica, poiché è lo sponsor che deve decidere quali funzioni intende fornire agli utenti e quali devono essere quindi valutate. ITSEC suggerisce di raccogliere le Funzioni di Sicurezza in otto categorie:

1. Identificazione e autenticazione. Sono tutte le funzioni relative all'identificazione e autenticazione di un utente che accede al sistema informatico.

2. Controllo degli accessi. Sono le funzioni che controllano il flusso di informazioni fra i processi del sistema informatico e il loro uso delle risorse.

3. Attribuibilità delle azioni (accountability). Sono le funzioni che tengono

traccia delle azioni delle varie entità (utenti o processi) in modo che esse possano essere attribuite a chi le ha compiute.

4. Ispezionabilità. Solo le funzioni che rilevano gli eventi del sistema che possono rappresentare una minaccia alla sicurezza del sistema stesso

5. Riutilizzo degli oggetti. Sono le funzioni il cui scopo è permettere la riutilizzazione di risorse del sistema senza che questo costituisca una minaccia per la sicurezza.

6. Accuratezza. Sono le funzioni che evitano le modifiche ai dati che ne possono minacciare l'integrità.

7. Affidabilità del servizio. Sono le funzioni che assicurano che le risorse siano accessibili entro tempi prefissati da parte di qualsiasi soggetto.

8. Scambio di dati. Sono le funzioni che garantiscono la sicurezza dei dati durante la loro trasmissione su canali di comunicazione non sicuri.

Le Funzioni di Sicurezza rappresentano il cuore di un Obiettivo di Sicurezza, poiché esse identificano le garanzie che sono fornite agli utenti. I due elementi restanti (l'efficacia e la correttezza) forniscono l'utente di un'adeguata fiducia nelle capacità del sistema di comportarsi secondo le proprie specifiche.

In particolare, la **valutazione dell'efficacia** delle Funzioni di Sicurezza intende stabilire se esse sono in grado di garantire la sicurezza del sistema informatico rispetto alle minacce previste. La **valutazione della correttezza** verifica invece se le funzioni di sicurezza siano state realizzate senza commettere errori che ne possono minare l'efficacia. In qualche modo, la valutazione dell'efficacia intende stabilire se il sistema così come è stato specificato è in grado di soddisfare i propri requisiti di sicurezza; la valutazione della correttezza intende invece stabilire se il sistema, così come è stato realizzato e messo in opera, risponde a tali requisiti.

È interessante notare la corrispondenza esistente fra lo standard ITSEC e i requisiti minimi di sicurezza. I requisiti minimi impongono un documento sulla sicurezza (equivalente in questo caso alla Politica di Sicurezza di Sistema) esclusivamente nel caso del trattamento di dati sensibili. Negli altri casi sono identificate Funzioni di Sicurezza (seppure non specificate come tali) relativamente all'identificazione e all'autenticazione, al controllo degli accessi, al riutilizzo degli oggetti e all'interconnessione. La specifica in questo caso è funzionale, ma non quantitativa: si identificano quali devono

essere le Funzioni di Sicurezza presenti nel sistema, ma non si fa alcuna specifica sul grado di efficacia e di correttezza degli stessi.

L'assenza di tali specifiche comporta che alcune delle misure di sicurezza identificate risultino onerose per chi le implementa e non adeguatamente efficaci. Un punto fortemente critico è rappresentato dalle parole chiavi che, secondo il requisito imposto dalle misure minime, devono essere utilizzate per l'accesso alle banche dati. Il requisito non fornisce alcuna indicazione sulla lunghezza minima di una parola chiave o sulla sua generazione; pertanto, parole chiavi come "pippo" sono perfettamente lecite. Poiché il problema identificato rientra all'interno della valutazione dell'efficacia e della correttezza delle Funzioni di Sicurezza, è utile approfondire ulteriormente la descrizione dello standard.

#### *4.3. La valutazione dell'efficacia*

Come già detto in precedenza, la valutazione dell'efficacia delle FS intende verificare che esse sono in grado di garantire gli obiettivi di sicurezza che l'Oggetto di Valutazione intende conseguire.

La valutazione dell'efficacia delle FS è svolta in due momenti distinti:

- Nella progettazione del sistema.
- Nella messa in opera del sistema.

La valutazione della progettazione del sistema intende verificare l'efficacia dei meccanismi, così come sono stati progettati, di resistere a un attacco diretto nei confronti del sistema. La valutazione dello sviluppo verifica quattro aspetti:

- La capacità delle FS di contrastare le minacce identificate nell'oggetto di sicurezza.
- La capacità delle FS di funzionare in modo sinergico.
- La capacità dei meccanismi di sicurezza che implementano le FS, di resistere ad attacchi diretti, in funzione delle risorse a disposizione dell'aggressore.
- La possibilità da parte delle vulnerabilità note di compromettere la sicurezza dell'oggetto di valutazione.

La valutazione della messa in opera del sistema intende verificare che il sistema non possa essere reso operativo in modo insicuro a insaputa dei suoi utenti. La valutazione della messa in opera del sistema verifica pertanto

due aspetti:

- La facilità di utilizzo delle FS.
- La possibilità da parte delle vulnerabilità note del sistema di compromettere la sicurezza dell'oggetto di valutazione.

Nel caso specifico in esame, è abbastanza chiaro come l'utilizzo di uno standard ITSEC avrebbe consentito di aumentare l'efficacia delle misure di sicurezza minime. In questo caso infatti la Funzione di Sicurezza di Identificazione degli Utenti, realizzata tramite un meccanismo di sicurezza di parola chiave, non avrebbe potuto essere valutata come efficace rispetto all'obiettivo di sicurezza di garantire l'accesso solo alle persone autorizzate: infatti, un utente con relativamente poche risorse avrebbe potuto tentare un attacco a vocabolario per cercare di identificare una parola chiave particolarmente breve o particolarmente semplice.

#### *4.4. La valutazione della correttezza*

La correttezza delle FS identifica la garanzia per l'utente finale che le FS siano state implementate correttamente: esse sono corrispondenti alle loro specifiche.

La correttezza è un aspetto critico del processo di sviluppo di un oggetto di valutazione, poiché una FS deve essere priva di problemi di implementazione per essere realmente efficace. Esistono numerosi casi di FS aggirabili, a causa della loro scorretta implementazione.

Poiché la correttezza è una proprietà negativa delle FS (è possibile dimostrare che un sistema ha un certo problema di sicurezza, ma non è possibile dimostrare che un sistema è sicuro dal punto di vista informatico), la correttezza delle FS viene certificata tramite l'ispezione del processo di sviluppo e della messa in opera dell'oggetto di valutazione. L'ispezione è strutturata per livelli successivi di complessità, e va da un livello E0 (corrispondente all'assenza di qualsiasi garanzia di correttezza) al livello E6 (corrispondente alla verifica formale di tutte le principali componenti per la garanzia della sicurezza).

Il livello di correttezza è l'ultimo (e non certamente il meno grave) fra gli elementi assenti nelle regole di sicurezza minime. La sua assenza non consente di stabilire la quantità di risorse che una PA deve dedicare per la garanzia di corretto utilizzo dei propri dati contenuti in sistemi informatici.

## 5. L'uso dello standard ITSEC nella PA

L'utilizzo dello standard ITSEC nella PA può essere particolarmente efficace con riferimento alle classi di Funzioni di Sicurezza, ossia alla possibilità di raccogliere i requisiti di sicurezza per sistemi simili in classi, e di definire per ciascuna classe quali siano le Funzioni di Sicurezza richieste, la forza dei meccanismi che le implementano e il livello di correttezza cui devono essere implementate.

L'uso di una classe consente di standardizzare i requisiti di sicurezza nel momento in cui essi diventano requisiti di sistemi da acquisire o da realizzare. Questo si traduce in un aumento dell'efficacia (poiché una specifica soluzione non deve essere realizzata su misura per un caso, ma è riprodotta e verificata in decine di installazioni) e in una corrispondente riduzione dei costi.

L'uso di una classe consente inoltre di effettuare due esami separati: un esame per verificare l'efficacia della classe e un esame per verificare la correttezza di implementazione di una classe da parte di un sistema. Il primo esame può essere condotto in pubblico, e vi possono partecipare tutti gli esperti del settore, al fine di garantire che la Classe di Funzioni che si definisce soddisfi le esigenze di sicurezza; il secondo esame è invece specifico di un prodotto o sistema, e può essere effettuato in modo separato ed indipendente.

Una volta identificato il concetto di classe, sorge immediatamente il problema di quali classi identificare per la privacy all'interno della PA. Una prima risposta può essere rappresentata dalle classi che emergono naturalmente dalla lettura delle misure di sicurezza minime. Esse possono essere distinte fra quelle relative al trattamento dei dati personali e quelle relative al trattamento dei dati sensibili, e a loro volta come segue:

1. Trattamento per fini personali.
2. Elaboratori stand-alone.
3. Elaboratori in rete non disponibile al pubblico.
4. Elaboratori in rete disponibile al pubblico.

Si hanno pertanto un totale di otto classi di funzionalità da definire. Come è già stato detto in precedenza, la normativa fornisce alcune indicazioni abbastanza precise relativamente ad alcune Funzioni di Sicurezza, ma è completamente carente sia nella specifica della forza dei meccanismi di sicurezza che implementano tali funzioni, sia nella loro correttezza di implementazione.

## 6. I problemi aperti

L'esame svolto fino a questo momento dello standard ITSEC ha evidenziato sia come esso possa essere efficace per definire i requisiti di riservatezza in termini chiari e non ambigui tanto per il Garante quanto per le P.P.A.A. chiamate ad attuare le relative misure di sicurezza.

Il primo problema relativo a tale standard è che a oggi l'Italia non ha ancora alcuna struttura di certificazione per sistemi ITSEC. L'Italia riconosce l'esistenza di tali standard, poiché li utilizza esplicitamente all'interno della normativa sulla firma digitale; tuttavia, lo stato italiano non ha ancora adottato esplicitamente la normativa ITSEC, ne' tantomeno ha costruito una struttura per la certificazione sul territorio italiano di sistemi ITSEC.

Un secondo e forse più importante problema è che le misure di sicurezza minime non fanno alcun accenno allo standard ITSEC, nè ad altro standard per la sicurezza dei sistemi. Pertanto, può essere discutibile la validità dell'esposizione fatta fino a questo momento, poiché essa può apparire come una costruzione assolutamente astratta.

Esistono tuttavia almeno due considerazioni che rendono questa parte dello studio comunque efficace. La prima e più semplice considerazione è che il regolamento è soggetto a una revisione periodica biennale, al fine di garantire il suo adeguamento con le mutate condizioni tecnologiche; dato che esiste in questo momento un forte interesse a livello internazionale verso gli standard per i sistemi di sicurezza (p.e., è stato definito da poco lo standard Common Criteria, che rappresenta sostanzialmente un'evoluzione dello standard ITSEC), è prevedibile che la realizzazione di sistemi sicuri e certificati aumenterà nel prossimo biennio.

La seconda considerazione è che come è già stato ricordato in precedenza, una classe di Funzioni di Sicurezza per ITSEC non costituirebbe uno stravolgimento delle misure di sicurezza minime, quanto piuttosto un loro completamento.

È pertanto accettabile pensare di definire Classi da utilizzare sia per la realizzazione di sistemi che per la loro verifica. Il loro utilizzo da parte di una PA potrebbe aiutare la PA ad acquisire fiducia di aver correttamente risposto ai requisiti di sicurezza minimi imposti, poiché essi sarebbero implementati tramite una Classe di Funzioni più generale, soggetta a pubblica revisione e collaudata in altre realtà. Inoltre, l'esistenza di requisiti standardizzati aiuta i produttori ad adeguare i loro prodotti alle specifiche esigenze di sicurezza, senza peraltro dover tentare pericolose interpretazioni della normativa vigente.



NORMATIVE STATALI



## NORMATIVE STATALI

Normative che istituiscono banche dati Errore. Il segnalibro non è definito.

*Legge 23 dicembre 1996, n. 662 (in Suppl. ordinario n. 233, alla Gazz. Uff. n. 303, del 28 dicembre 1996).* - *Misure di razionalizzazione della finanza pubblica.*

*Decreto-legge 18 dicembre 1995, n. 532 (in Gazz. Uff., 19 dicembre, n. 295).*  
*-Disposizioni urgenti per le attività produttive.*

*Decreto Ministeriale 2 febbraio 1994, n. 285 (in Gazz. Uff., 13 maggio, n. 110).* - *Regolamento recante i criteri, le procedure e le modalità di utilizzazione della quota del dieci per cento del Fondo nazionale per l'artigianato.*

*Decreto Ministeriale 6 ottobre 1990, n. 460 (in Gazz. Uff., 7 agosto, n. 184).* - *Regolamento recante organizzazione della Direzione generale della difesa del suolo.*

## NORMATIVE CHE ISTITUISCONO BANCHE DATI E NE DISCIPLINANO L'ACCESSO E LE MODALITÀ DI ACQUISIZIONE DI DATI

*Decreto-legge 17 maggio 1996, n. 263 (in Gazz. Uff., 18 maggio, n. 115).*  
*- Disposizioni fiscali urgenti in materia di controlli e anagrafe patrimoniale dei dipendenti, al fine di contrastare l'evasione e la corruzione.*

*Legge 5 gennaio 1994, n. 36 (in Suppl. ordinario n. 11, alla Gazz. Uff. n. 14, del 19 gennaio).* - *Disposizioni in materia di risorse idriche. (GALLI).*

Normative che istituiscono banche dati, fanno riferimento a banche dati esistenti, ne prevedono l'accesso e ne disciplinano l'interconnessione.

*Decreto Ministeriale 15 dicembre 1995, n. 592 (in Gazz. Uff., 30 maggio, n. 125).* - *Regolamento concernente il piano nazionale per la eradicazione della tubercolosi negli allevamenti bovini e bufalini.*

*Decreto del Presidente della Repubblica 7 dicembre 1995, n. 581 (in Suppl. ordinario n. 17, alla Gazz. Uff. n. 28, del 3 febbraio).* - *Regolamento di attuazione dell'art. 8 della legge 29 dicembre 1993, n. 580, in materia di istituzione del registro delle imprese di cui all'art. 2188 del codice civile.*

*Decreto Ministeriale 27 dicembre 1994, n. 762 (in Gazz. Uff., 13 febbraio, n. 36).*  
*- Regolamento recante ulteriori disposizioni per l'applicazione delle quote latte.*

*Decreto-legge 18 luglio 1994, n. 452 (in Gazz. Uff., 19 luglio, n. 167). - Disposizioni fiscali urgenti in materia di accertamento, contenzioso, potenziamento degli organici, controlli e anagrafe patrimoniale dei dipendenti, al fine di contrastare l'evasione e la corruzione.*

*Decreto del Presidente della Repubblica 5 aprile 1993, n. 106 (in Gazz. Uff., 10 aprile, n. 84). - Regolamento concernente la riorganizzazione ed il potenziamento dei Servizi tecnici nazionali nell'ambito della Presidenza del Consiglio dei Ministri, ai sensi dell'art. 9 della legge 18 maggio 1989, n. 183.*

*Decreto Ministeriale 2 ottobre 1992, n. 514 (in Gazz. Uff., 31 dicembre, n. 306). - Regolamento sulle modalità e le procedure concernenti il funzionamento degli uffici del pubblico registro automobilistico, la tenuta degli archivi, la conservazione della documentazione prescritta, la elaborazione e fornitura dei dati e delle statistiche dei veicoli iscritti, la forma, il contenuto e le modalità di utilizzo della modulistica occorrente per il funzionamento degli uffici medesimi, nonché i tempi di attuazione delle nuove procedure, in attuazione dell'art. 7 della legge 9 luglio 1990, n. 187.*

*Decreto del Presidente della Repubblica 24 gennaio 1991, n. 85 (in Gazz. Uff., 18 marzo, n. 65). - Regolamento concernente la riorganizzazione ed il potenziamento dei Servizi tecnici nazionali geologico, idrografico e mareografico, sismico e dighe nell'ambito della Presidenza del Consiglio dei Ministri, ai sensi dell'art. 9 della legge 18 maggio 1989, n. 183. [testo REGOLAMENTO] [parte 2 di 2]*

*Decreto legislativo 26 aprile 1990, n. 105 (in Suppl. ordinario alla Gazz. Uff. n. 106, del 9 maggio). - Organizzazione centrale e periferica dell'Amministrazione delle dogane e delle imposte indirette e ordinamento del relativo personale, in attuazione della legge 10 ottobre 1989, n. 349.*

*Decreto legislativo 6 settembre 1989, n. 322 (in Gazz. Uff., 22 settembre, n. 222). - Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'art. 24 della legge 23 agosto 1988, n. 400.*

Normative che fanno riferimento a banche dati esistenti.

*D.P.C.M. 4 marzo 1998 (1). (in Gazz. Uff. 27 luglio 1998, n. 173) Individuazione dei criteri e dei parametri per la valutazione del numero complessivo dei dipendenti in servizio nelle amministrazioni dello Stato, anche ad ordinamento autonomo, ai sensi dell'art. 39, comma 2, della L. 27 dicembre 1997, n. 449 .*

*Decreto del Presidente della Repubblica 20 febbraio 1998, n. 38 (in Gazz. Uff., 11 marzo, n. 58). - Regolamento recante le attribuzioni dei Dipartimenti del Ministero del tesoro, del bilancio e della programmazione economica, nonché disposizioni in materia di organizzazione e di personale, a norma dell'art. 7, comma 3, della legge 3 aprile 1997, n. 94.*

*Legge 30 dicembre 1997, n. 458 (in Gazz. Uff., 2 gennaio, n. 1). - Interventi urgenti per il potenziamento delle strutture, delle attrezzature e dei servizi dell'Amministrazione della giustizia.*

*Legge 5 febbraio 1992, n. 81 (in Gazz. Uff., 14 febbraio, n. 37). - Disposizioni sull'aggiornamento dell'aggio ai rivenditori dei generi di monopolio, sul finanziamento dell'ATI - Azienda tabacchi italiani S.p.a., sul completamento della informatizzazione dell'Amministrazione autonoma dei monopoli di Stato, nonché in ordine alla esclusione dei tabacchi lavorati dagli indici dei prezzi al consumo e dall'indice sindacale per la contingenza.*

Normative che fanno riferimento a banche dati esistenti e disciplinano l'obbligo di fornire dati.

*O.M. 20 maggio 1997 (in Gazz. Uff. 24 maggio 1997, n. 119).*

*Misure urgenti per la rilevazione straordinaria dei capi bovini presenti nelle aziende da latte.*

*Decreto del Presidente del Consiglio dei Ministri 10 febbraio 1984 (in Gazz. Uff., 24 febbraio, n. 55). - Indirizzo e coordinamento dell'attività amministrativa delle regioni in materia di requisiti minimi di strutturazione, di dotazione strumentale e di qualificazione funzionale del personale dei presidi che erogano prestazioni di diagnostica di laboratorio.*

*Decreto Ministeriale 23 maggio 1995 (in Gazz. Uff., 1° giugno, n. 126). - Indicazione dei dati che il sistema informativo del Ministero delle finanze trasmette al sistema informativo del Ministero del tesoro - Ragioneria generale dello Stato, relativamente alle contabilità tenute dai concessionari sui conti fiscali. Modalità, termini e caratteristiche tecniche di trasmissione dei dati stessi.*

*Decreto Ministeriale 4 aprile 1995 (in Gazz. Uff., 11 aprile, n. 85). (del Direttore generale della motorizzazione civile e dei trasporti in concessione) - Modalità di collegamento telematico per la trasmissione alla Direzione generale della motorizzazione civile e dei trasporti in concessione delle certificazioni relative alle revisioni effettuate da imprese, consorzi o società consortili.*

*Decreto del Presidente della Repubblica 4 giugno 1997, n. 335 (in Gazz. Uff., 6 ottobre, n. 233). - Regolamento concernente la disciplina delle modalità di organizzazione dell'Agenzia nazionale per la protezione dell'ambiente in strutture operative..*

*D.P.R. 28 settembre 1994, n. 634 (in Gazz. Uff. 19 novembre 1994, n. 271).*

*Regolamento per l'ammissione all'utenza del servizio di informatica del centro di elaborazione dati della Direzione generale della motorizzazione civile e dei trasporti in concessione.*

*D.P.R. 13 marzo 1986, n. 156. (in Gazz. Uff. 13 maggio 1986, n. 109)*

*Regolamento per l'ammissione all'utenza del servizio di informatica del centro elaborazione dati della Direzione generale della motorizzazione civile e dei trasporti in concessione.*

Normative che fanno riferimento a banche dati esistenti e prevedono l'accesso da parte di soggetti diversi.

*D.M. 22 giugno 1998 (in Gazz. Uff. 27 giugno 1998, n. 148).*

*Modificazioni alle modalità per lo svolgimento degli accertamenti in materia di produzione lattiera.*

*L. 27 dicembre 1997, n. 449 (in Gazz. Uff. 30 dicembre 1997, n. 302, S.O).Misure per la stabilizzazione della finanza pubblica.*

*D.M. 24 dicembre 1997 (in Gazz. Uff. 2 gennaio 1998, n. 1).*

*Programmazione dei flussi migratori per l'anno 1998.*

*Decreto legislativo 19 novembre 1997, n. 414 (in Gazz. Uff., 2 dicembre, n. 282). - Attività informatiche dell'Amministrazione statale in materia finanziaria e contabile.*

*Decreto del Presidente della Repubblica 6 febbraio 1996, n. 102 (in Gazz. Uff., 2 marzo, n. 52). - Regolamento recante norme sulla Cabina di regia nazionale.*

*Decreto legislativo 21 settembre 1995, n. 429 (in Gazz. Uff., 19 ottobre, n. 245). - Norme di attuazione dello statuto speciale della Regione Trentino-Alto Adige recanti delega di funzioni amministrative alle province autonome di Trento e di Bolzano in materia di comunicazioni e trasporti.*

*Decreto-legge 27 marzo 1995, n. 87 (in Gazz. Uff., 28 marzo, n. 73). --*

*Istituzione dell'Ente per gli interventi nel mercato agricolo - E.I.M.A.*

*Decreto legislativo 17 marzo 1995, n. 230 (in Suppl. ordinario n. 74, alla Gazz. Uff. n. 136, del 13 giugno). - Attuazione delle direttive Euratom 80/836, 84/467, 84/466, 89/618, 90/641 e 92/3 in materia di radiazioni ionizzanti.*

*Decreto Ministeriale 30 dicembre 1993 (in Suppl. ordinario n. 4, alla Gazz. Uff. n. 5, del 8 gennaio). - Apertura e aggiornamento dei conti fiscali.*

*Decreto-legge 15 gennaio 1993, n. 6 (in Gazz. Uff., 16 gennaio, n. 12). - Disposizioni urgenti per il recupero degli introiti contributivi in materia previdenziale.*

*D.Lgs. 31 dicembre 1992, n. 545.*

*Ordinamento degli organi speciali di giurisdizione tributaria ed organizzazione degli uffici di collaborazione in attuazione della delega al Governo contenuta nell'art. 30 della legge 30 dicembre 1991, n. 413.*

*Legge 29 dicembre 1990, n. 407 (in Gazz. Uff., 31 dicembre, n. 303). - Disposizioni diverse per l'attuazione della manovra di finanza pubblica 1991-1993.*

*Normative che concernono le Camere di Commercio, istituendo banche dati, prevedendone l'accesso, nonché l'interconnessione da parte di altri soggetti.*

*Decreto Ministeriale 16 dicembre 1997, n. 486 (in Gazz. Uff., 19 gennaio, n. 14). - Regolamento recante norme per lo snellimento delle procedure in materia di comunicazioni antimafia.*

*Decreto-legge 25 marzo 1997, n. 67 (in Gazz. Uff., 26 marzo, n. 71). - Disposizioni urgenti per favorire l'occupazione.*

*Decreto Ministeriale 4 novembre 1993, n. 573 (in Suppl. ordinario n. 2, alla Gazz. Uff. n. 3, del 5 gennaio). -- Regolamento recante norme di attuazione della legge 5 febbraio 1992, n. 169, per la disciplina del riconoscimento delle denominazioni di origine, dell'albo degli oliveti, della denuncia di produzione delle olive e dell'attività delle commissioni di degustazione degli oli a denominazione di origine controllata.*

*Normative di derivazione comunitaria che istituiscono banche dati.*

*D.Lgs. 16 luglio 1998, n. 285 (in Gazz. Uff. 18 agosto 1998, n. 191).*

*Attuazione di direttive comunitarie in materia di classificazione, imballaggio ed etichettatura dei preparati pericolosi, a norma dell'articolo 38 della L. 24*

aprile 1998, n. 128.

*Decreto-legge 13 settembre 1996, n. 477 (in Gazz. Uff., 16 settembre, n. 217). - Disposizioni urgenti in materia di politica dell'immigrazione e per la regolamentazione dell'ingresso e soggiorno nel territorio nazionale dei cittadini dei Paesi non appartenenti all'Unione europea.*

Normative di derivazione comunitaria che fanno riferimento a banche dati esistenti.

*Decreto del Presidente della Repubblica 29 dicembre 1988, n. 568 (in Gazz. Uff., 1° febbraio, n. 26). - Approvazione del regolamento per l'organizzazione e le procedure amministrative del Fondo di rotazione per l'attuazione delle politiche comunitarie, in esecuzione dell'art. 8 della legge 16 aprile 1987, n. 183. [testo REGOLAMENTO]*

Normative enti locali.

Normative che istituiscono banche dati, e/o ne disciplinano l'accesso, e/o prevedono l'interconnessione con altre banche dati esistenti.

*Decreto legislativo 23 dicembre 1997, n. 469 (in Gazz. Uff., 8 gennaio, n. 5). - Conferimento alle regioni e agli enti locali di funzioni e compiti in materia di mercato del lavoro, a norma dell'art. 1 della legge 15 marzo 1997, n. 59.*

*Decreto legislativo 28 agosto 1997, n. 281 (in Gazz. Uff., 30 agosto, n. 202). - Definizione ed ampliamento delle attribuzioni della Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e Bolzano ed unificazione, per le materie ed i compiti di interesse comune delle regioni, delle province e dei comuni, con la Conferenza Stato-città ed autonomie locali.*

*L. 15 maggio 1997, n. 127 - Misure urgenti per lo snellimento dell'attività amministrativa e dei procedimenti di decisione e di controllo.*

*Legge 15 marzo 1997, n. 59 (in Suppl. ordinario n. 56/L, alla Gazz. Uff. n. 63, del 17 marzo). - Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa.*

*Legge 23 dicembre 1996, n. 662 (in Suppl. ordinario n. 233, alla Gazz. Uff. n. 303, del 28 dicembre 1996). - Misure di razionalizzazione della finanza pubblica.*

*Legge 11 gennaio 1996, n. 23 (in Gazz. Uff., 19 gennaio, n. 15). - Norme*

*per l'edilizia scolastica.*

*D.M. 1° marzo 1996. - Istituzione della banca dati degli organi di revisione economico-finanziaria degli enti locali.*

*Decreto Ministeriale 15 dicembre 1995, n. 592 (in Gazz. Uff., 30 maggio, n. 125). - Regolamento concernente il piano nazionale per la eradicazione della tubercolosi negli allevamenti bovini e bufalini.*

*Decreto del Presidente del Consiglio dei Ministri 5 maggio 1994 (in Gazz. Uff., 27 giugno, n. 148). - Modalità tecniche e ripartizione delle spese connesse alla realizzazione di collegamenti telematici tra comuni ed organismi che esercitano attività di prelievo contributivo e fiscale o erogano servizi di pubblica utilità.*

*Legge 5 gennaio 1994, n. 36 (in Suppl. ordinario n. 11, alla Gazz. Uff. n. 14, del 19 gennaio). - Disposizioni in materia di risorse idriche. (GALLI).*

*Decreto legislativo 3 febbraio 1993, n. 29 (in Suppl. ordinario alla Gazz. Uff., 6 febbraio, n. 30). - Razionalizzazione dell'organizzazione delle amministrazioni pubbliche e revisione della disciplina in materia di pubblico impiego.*

*Decreto del Presidente della Repubblica 5 aprile 1993, n. 106 (in Gazz. Uff., 10 aprile, n. 84). - Regolamento concernente la riorganizzazione ed il potenziamento dei Servizi tecnici nazionali nell'ambito della Presidenza del Consiglio dei Ministri, ai sensi dell'art. 9 della legge 18 maggio 1989, n. 183.*

*Legge 30 dicembre 1991, n. 413 (in Suppl. ordinario alla Gazz. Uff. n. 305, del 31 dicembre 1991). - Disposizioni per ampliare le basi imponibili, per razionalizzare, facilitare e potenziare l'attività di accertamento; disposizioni per la rivalutazione obbligatoria dei beni immobili delle imprese, nonchè per riformare il contenzioso e per la definizione agevolata dei rapporti tributari pendenti; delega al Presidente della Repubblica per la concessione di amnistia per reati tributari; istituzioni dei centri di assistenza fiscale e del conto fiscale.*

*Decreto legislativo 6 settembre 1989, n. 322 (in Gazz. Uff., 22 settembre, n. 222). - Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'art. 24 della legge 23 agosto 1988, n. 400.*

*Decreto Ministeriale 20 maggio 1991 (in Gazz. Uff., 31 maggio, n. 126). - Criteri per la raccolta dei dati inerenti la qualità dell'aria.*

*Legge 18 maggio 1989, n. 183 (in Suppl. ordinario alla Gazz. Uff., n. 120, del 25 maggio). - Norme per il riassetto organizzativo e funzionale della difesa del suolo.*

Normative che istituiscono banche dati e disciplinano l'obbligo di fornire dati.

L. 19 marzo 1993, n. 68. - Disposizioni urgenti in materia di finanza derivata e di contabilità pubblica.

*Decreto Ministeriale 20 maggio 1991 (in Gazz. Uff., 30 dicembre, n. 304). - Approvazione del regolamento del servizio informativo-telematico. [testo REGOLAMENTO].*

Normative che fanno riferimento a banche dati esistenti e ne prevedono l'accesso.

*D.P.R. 23 marzo 1998, n. 138. Regolamento recante norme per la revisione generale delle zone censuarie, delle tariffe d'estimo delle unità immobiliari urbane e dei relativi criteri nonché delle commissioni censuarie in esecuzione dell'articolo 3, commi 154 e 155, della L. 23 dicembre 1996, n. 662.*

*D.P.C.M. 4 marzo 1998. - Individuazione dei criteri e dei parametri per la valutazione del numero complessivo dei dipendenti in servizio nelle amministrazioni dello Stato, anche ad ordinamento autonomo, ai sensi dell'art. 39, comma 2, della L. 27 dicembre 1997, n. 449.*

*Decreto legislativo 15 dicembre 1997, n. 446 (in Suppl. ordinario n. 252/L, alla Gazz. Uff. n. 298, del 23 dicembre 1997). - Istituzione dell'imposta regionale sulle attività produttive, revisione degli scaglioni, delle aliquote e delle detrazioni dell'Irpef e istituzione di una addizionale regionale a tale imposta, nonché riordino della disciplina dei tributi locali.*

*Decreto legislativo 23 dicembre 1993, n. 546 (in Suppl. ordinario n. 123, alla Gazz. Uff. n. 304, del 29 dicembre 1993). - Ulteriori modifiche al decreto legislativo 3 febbraio 1993, n. 29, sul pubblico impiego.*

*Decreto legislativo 15 dicembre 1997, n. 446 (in Suppl. ordinario n. 252/L, alla Gazz. Uff. n. 298, del 23 dicembre 1997). - Istituzione dell'imposta regionale sulle attività produttive, revisione degli scaglioni, delle aliquote e delle detrazioni dell'Irpef e istituzione di una addizionale regionale a tale imposta, nonché riordino della disciplina dei tributi locali.*

*Decreto Ministeriale 13 dicembre 1991 (in Gazz. Uff., 4 gennaio, n. 3). - Direttive per la redazione, elaborazione, aggiornamento e trasmissione della mappatura relativa agli impianti di acquedotto e per la trasmissione dei dati relativi ai controlli analitici esperiti sulle acque destinate al consumo umano.*

*Decreto legislativo 12 luglio 1991, n. 212 (in Gazz. Uff., 18 luglio, n. 167). - Disciplina delle modalità di accesso delle amministrazioni pubbliche al sistema informativo dell'anagrafe tributaria.*

Normative che fanno riferimento a banche dati esistenti e disciplinano l'obbligo di fornire i dati o le modalità di acquisizione.

*Decreto legislativo 15 dicembre 1997, n. 446 (in Suppl. ordinario n. 252/L, alla Gazz. Uff. n. 298, del 23 dicembre 1997). - Istituzione dell'imposta regionale sulle attività produttive, revisione degli scaglioni, delle aliquote e delle detrazioni dell'Irpef e istituzione di una addizionale regionale a tale imposta, nonché riordino della disciplina dei tributi locali.*

*Decreto del Presidente della Repubblica 4 giugno 1997, n. 335 (in Gazz. Uff., 6 ottobre, n. 233). - Regolamento concernente la disciplina delle modalità di organizzazione dell'Agenzia nazionale per la protezione dell'ambiente in strutture operative.*

*O.M. 20 maggio 1997 (in Gazz. Uff. 24 maggio 1997, n. 119).- Misure urgenti per la rilevazione straordinaria dei capi bovini presenti nelle aziende da latte.*

*Decreto Ministeriale 5 dicembre 1996 (in Gazz. Uff., 20 dicembre, n. 298). - Approvazione dei termini e delle modalità per l'interscambio fra i comuni ed il sistema informativo del Ministero delle finanze dei dati e delle notizie delle dichiarazioni relative all'imposta comunale sugli immobili (ICI) dovuta per l'anno 1995.*

*Decreto legislativo 3 marzo 1993, n. 123 (in Gazz. Uff., 27 aprile, n. 97). - Attuazione della direttiva 89/397/CEE relativa al controllo ufficiale dei prodotti alimentari.*

Normative che fanno riferimento a banche dati, ne prevedono l'accesso e l'interconnessione.

*Decreto legislativo 3 febbraio 1993, n. 29 (in Suppl. ordinario alla Gazz. Uff., 6 febbraio, n. 30). - Razionalizzazione dell'organizzazione delle amministrazioni pubbliche e revisione della disciplina in materia di pubblico impiego.*

*Decreto legislativo 30 dicembre 1992, n. 504 (in Suppl. ordinario alla Gazz. Uff., 30 dicembre 1992, n. 305). - Riordino della finanza degli enti territoriali, a norma dell'art. 4 della legge 23 ottobre 1992, n. 421.*

*Decreto Ministeriale 18 giugno 1991 (in Gazz. Uff., 18 luglio, n. 167). - Indicazioni per l'istituzione del registro del sangue in ciascuna regione e provincia autonoma.*

*Legge 12.11.1990 n. 331 (in Gazz. Uff., 19 settembre, n. 219). - Disposizioni fiscali urgenti in materia di finanza locale, di accertamenti in base ad elementi segnalati dall'anagrafe tributaria e disposizioni per il contenimento del disavanzo del bilancio dello Stato.*

*Decreto legislativo 3 marzo 1993, n. 123 (in Gazz. Uff., 27 aprile, n. 97). - Attuazione della direttiva 89/397/CEE relativa al controllo ufficiale dei prodotti alimentari.*

*Decreto Ministeriale 27 settembre 1989 (in Gazz. Uff., 30 settembre, n. 229). - Modalità per la predisposizione delle richieste di chiarimenti, la trasmissione degli elenchi ai comuni e dei dati tra gli uffici finanziari ai fini degli accertamenti dei redditi dei fabbricati.*

Normative che fanno riferimento a banche dati esistenti e disciplinano l'obbligo di fornire dati, prevedendo, in caso di inadempienza, apposite sanzioni.

*Legge 27 dicembre 1997, n. 449 (in Suppl. ordinario n. 255/L, alla Gazz. Uff. n. 302, del 30 dicembre 1997). - Misure per la stabilizzazione della finanza pubblica..*

*Legge 17 marzo 1993, n. 63 (in Gazz. Uff., 18 marzo, n. 64). - Disposizioni urgenti per il recupero degli introiti contributivi in materia previdenziale.*

Normative di derivazione comunitaria che istituiscono banche dati..

*Legge 28 marzo 1997, n. 81 (in Gazz. Uff., 1° aprile, n. 75). - Conversione in legge, con modificazioni, del decreto-legge 31 gennaio 1997, n. 11, recante misure straordinarie per la crisi del settore lattiero-caseario ed altri interventi urgenti a favore dell'agricoltura.*

Normative di derivazione comunitaria che fanno riferimento a banche dati esistenti.

*Decreto Ministeriale 19 febbraio 1991, n. 63 (in Gazz. Uff., 2 marzo, n. 52).*

- *Regolamento recante disposizioni di adattamento alla realtà nazionale del regime di aiuti per il ritiro di seminativi dalla produzione di cui al regolamento CEE del Consiglio delle Comunità europee n. 797/85.*

Normativa concernente la rete unitaria della pubblica amministrazione

*Direttiva del Presidente del Consiglio dei Ministri 5 settembre 1995 (in Gazz. Off., 21 novembre, n. 272). - Principi e modalità per la realizzazione della Rete unitaria della pubblica amministrazione.*

NORMATIVE REGIONE TOSCANA

*L.R. 4 aprile 1997, n. 26.*

*Norme di indirizzo per l'organizzazione del servizio idrico integrato in attuazione degli articoli 11 e 12 della legge 5 gennaio 1994, n. 36.*

*Dec.G.R. 20 maggio 1996, n. 1.*

*Circolare esplicativa della L.R. 15 marzo 1996, n. 18. "Ordinamento del Bollettino Ufficiale della Regione Toscana e norme per la pubblicazione degli atti".*

*L.R. 2 maggio 1996, n. 35.*

*Interventi in materia di servizio civile.*

*Reg. 7 marzo 1995.*

*Regolamento Interno degli Uffici del Consiglio regionale.*

*Delib.C.R. 25 luglio 1994, n. 348 .*

*Direttiva ai Comuni e alle Unità Sanitarie Locali per la costituzione e il funzionamento del servizio per l'affidamento familiare.*

*L.R. 30 dicembre 1992, n. 62.*

*Prime norme per la formazione dei piani per il coordinamento degli orari degli esercizi commerciali, dei servizi pubblici e degli uffici periferici delle amministrazioni pubbliche. Finanziamento dell'attività di ricerca da parte dei Comuni singoli o associati (1).*

*L.R. 7 luglio 1992, n. 31.*

*Disciplina del controllo sugli atti degli enti locali.*

*L.R. 12 agosto 1991, n. 41.*

*Esercizio delle competenze regionali in materia di rischi di incidenti rilevanti*

*di cui al D.P.R. 17 maggio 1988, n. 175.*

*Delib.C.R. 8 maggio 1991, n. 125 .*

*L.R. n. 46 del 1989 art. 1 - Approvazione documento indirizzi per le strategie del risparmio di energia e di sviluppo fonti rinnovabili.*

*Reg. 18 gennaio 1991, n. 1.*

*Centro Regionale documentazione - C.E.D.O.C. - Disciplina per le attività organizzative e per l'esercizio delle funzioni ai sensi art. 72 della L.R. 9 aprile 1990, n. 38 (1).*

*L.R. 19 agosto 1988, n. 60.*

*Norme per la limitazione ed il recupero dei rifiuti (1).*

*L.R. 21 marzo 1988, n. 20.*

*Interventi regionali a favore della cooperazione agricola e forestale.*

*Disciplina regionale degli scarichi delle pubbliche fognature e degli insediamenti civili che non recapitano in pubbliche fognature (Art. 14 L. 319/1976).*

*Delib.C.R. 31 marzo 1998, n. 77.*

*Direttive di attuazione del piano di indirizzo degli interventi di qualificazione dell'offerta turistica.*

*Reg. 9 novembre 1994.*

*Regolamento interno approvato dal Consiglio regionale della Toscana nella seduta del 9 novembre 1994 relativo al "Diritto di accesso alle informazioni e ai documenti amministrativi del Consiglio regionale".*

*L.R. 7 luglio 1992, n. 31.*

*Disciplina del controllo sugli atti degli enti locali.*

*L.R. 19 dicembre 1996, n. 95.*

*Disciplina degli interventi per lo sviluppo della montagna.*

*Reg. 10 settembre 1996, n. 7.*

*Disciplina delle attività di valutazione dei risultati delle strutture dirigenziali e delle prestazioni dei dirigenti regionali (art. 24 L.R. 7 novembre 1994, n. 81).*

*L.R. 7 novembre 1994, n. 81.*

*Recepimento del decreto legislativo 3 febbraio 1993, n. 29. Modifiche all'ordinamento della dirigenza e della struttura operativa regionale (1).*

*Delib.C.R. 14 ottobre 1997, n. 335.(1).*

*L.R. 2 settembre 1992, n. 43 - artt. 3 e 6 - Approvazione del "programma statistico regionale 1997-1999" e presa d'atto del "Rapporto sull'attività svolta nell'anno 1996".*

*Programma statistico regionale 1997-1999.*

*Rapporto sull'attività svolta nel 1996.*